

APOGEE *Communications*

Rapport de
Veille Technologique Sécurité
N°57

Avril 2003

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: mailing-lists, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Les symboles d'avertissement suivants seront éventuellement utilisés:

- Site dont la consultation est susceptible de générer directement ou indirectement, une attaque sur l'équipement de consultation, voire de faire encourir un risque sur le système d'information associé.
- Site susceptible d'héberger des informations ou des programmes dont l'utilisation est répréhensible au titre de la Loi Française.

Aucune garantie ne peut être apportée sur l'innocuité de ces sites, et en particulier, sur la qualité des applets et autres ressources présentées au navigateur **WEB**.

La diffusion de ce document est restreinte aux clients des services VTS-RAPPORT et VTS_ENTREPRISE

APOGEE Communications
1, Rue Jean Rostand
91893 ORSAY CEDEX

Pour tous renseignements
Offre de veille: http://www.apogee-com.fr/veille
Informations: vts-info@apogee-com.fr



Au sommaire de ce rapport …





Le mot de la rédaction ...

Le 24 avril, Microsoft dévoilait Windows Server 2003 avec la promesse de fournir un système '3D' c'est à dire sécurisé par sa conception ("secure by **D**esign"), sécurisé par défaut ("secure by **D**efault") et sécurisé dans son déploiement ("secure in **D**eployment").

Nous conseillons fortement la lecture d'un très intéressant article qui tente de faire le point à ce sujet. Celui-ci, publié dans le numéro d'avril du magazine '**InfoSecurityMag**', est accessible via l'URL http://www.infosecuritymag.com/2003/apr/cover.shtml.

L'équipe de Veille Technologique



PRODUITS ET TECHNOLOGIES

LES PRODUITS

AUDIT

NMAP V3.20 / V3.25

▪ **Description**

L'utilitaire '**Network Mapper**', plus connu sous le nom '**Nmap**' (Rapport N°42 – Août 2002), vient de subir une cure de jouvence portant aussi bien sur les fonctionnalités embarquées que sur les performances sans oublier l'adjonction ou la mise à jour de plus de **161** empreintes dans la base des équipements détectés.

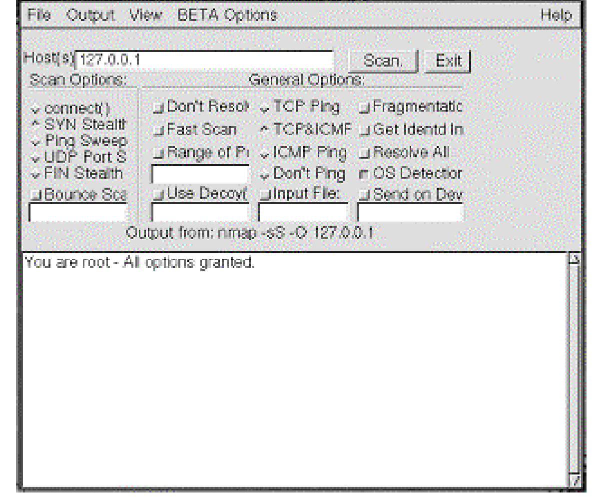
Rappelons que ' **Nmap**' permet non seulement d'inventorier les équipements actifs d'un réseau par un sondage (ou '**scan**' dans le jargon) selon une stratégie configurable mais aussi d'identifier ceux-ci par analyse des drapeaux et autres éléments protocolaires contenus dans les différents paquets de réponse. Il est très largement utilisé et s'est imposé comme un outil de sondage incontournable aussi bien pour les plates-formes UNIX que les plates-formes WIN32.

Il propose en effet différentes méthodes de sondage de ports:

- le classique sondage '**TCP CONNECT**'
- le sondage '**TCP SYN**' (aucune connexion n'est établie donc rien n'est journalisé au niveau des services testés)
- les sondages '**TCP ACK**' et '**TCP WINDOW**' (ce qui permet de mettre en évidence la présence de firewall sans état)
- le sondage '**UDP**' classique
- le sondage TCP par rebond via un serveur FTP
- le sondage de RPC
- le sondage '**TCP CONNECT**' avec identification de l'utilisateur qui fait tourner le service testé.
- le sondage '**IDLE**' ou '**zombie scan**' permettant un anonymat complet vis à vis de la cible.

En plus de ces différentes méthodes de sondages, '**Nmap**' est capable de déterminer les protocoles activés sur la cible.

'**Nmap**' est enfin capable d'identifier le système d'exploitation d'une machine distante en employant une technique connue sous le nom de prise d'empreinte de pile TCP. Cette technique tire parti du fait que toutes les implémentations IP n'ont pas les mêmes réactions lors de la réception de requêtes non valides. La connaissance de la réaction de chaque système permet d'identifier celui-ci avec un taux d'erreur raisonnable.



'**Nmap**' dispose d'une interface graphique pour plates formes **WIN32** et **UNIX**. Il se compile également dans ces deux environnements. Notons toutefois que la version **WIN32** de '**Nmap**' utilise l'interface d'accès **WinPcap** tandis que la version Unix utilise l'interface '**libpcap**'.

Parmi les nouveautés présentes dans la version 3.2x, en dehors d'un bon nombre de corrections de problèmes, on trouve les points suivants:

- la réécriture d'une bonne partie du code en langage C++,
- l'ajout du support du protocole **IP V6** pour certaines plates-formes et certaines méthodes de sondages,
- la possibilité de définir le '**TTL**' (Time To Live) des paquets transmis,
- l'amélioration des algorithmes utilisés par les méthodes de sondage '**WINDOW**', '**CONNECT**' et '**SYN TCP**' conduisant à de meilleures performances,
- l'ajout d'un nombre important de signatures de systèmes d'exploitation,

Le paquetage '**Nmap**' est livré avec quatre fichiers de référence que l'utilisateur pourra éventuellement modifier ou mettre à jour:

- '**nmap-os-fingerprint**':
  Véritable clef de voûte de l'application, ce fichier contient les signatures mises à jour de quelques **866** équipements et systèmes réseaux (contre **705** dans la version V3.00).
- '**nmap-services**':
  Ce fichier contient la description des services pour chacun des numéros de ports qui y sont référencés soit **2172** services dans la version actuelle (contre **2149** services dans la version 3.0).
- '**nmap-rpc**':



Ce fichier contient la liste des numéros des programmes **SUN RPC** connus dans un format identique à celui du fichier '**rpc**' sous UNIX soit **451** programmes.

- '**nmap-protocols**':
  Ce fichier contient la description de quelques 129 numéros de protocoles IP enregistrés (**UDP**, **TCP** et **ICMP** ne sont que trois protocoles **IP** parmi 255 possibles).

On notera que durant la période de test de la version '**3.20**', trois nouvelles versions sont apparues: '**Nmap V3.21**' devenue par la suite '**Nmap V3.23**', '**Nmap V3.25**' puis '**Nmap V3.26**'. En dehors de l'implémentation d'une nouvelle méthode de sondage '**UDP**' dite '**ping scan UDP**', le reste des modifications concerne la correction de problèmes d'importance variable.

- **Complément d'information**

http://www.insecure.org/nmap/nmap_download.html

LES TECHNOLOGIES

INTRUSION

RESULTAT DU CONCOURS HONEYD

- **Description**

Le 17 février 2003, **Niels Provost**, l'auteur du logiciel libre '**honeyd**', lançait un concours dénommé '**Honeyd challenge**' visant à améliorer les fonctionnalités de ce logiciel. Rappelons que celui-ci permet de recréer un environnement de systèmes et d'équipements purement virtuels. Il est ainsi possible d'observer et d'étudier le comportement de systèmes tiers et les attaques en provenance de ceux-ci sans risquer de compromettre un système réel.

Le 31 mars, les résultats de ce concours – et les développements associés - ont été publiés. Ont été ainsi proposées et développées les fonctionnalités suivantes:

'**Honeycomb**' Ce module additionnel permet de générer automatiquement des signatures au format '**snort**' correspondant aux tentatives d'attaque détectées sur le pot de miel '**honeyd**'. On notera que la mise en place de ce module requiert quelques modifications dans le code original du pot de miel '**honeyd**'.

'**RandomNet**' Cet utilitaire permet de générer de manière simple, aléatoire et réaliste les fichiers de configuration du pot de miel '**honeyd**'. Entièrement écrit en Java, '**RandomNet**' pourra être exécuté dans de nombreux environnements. Un manuel d'utilisation complet est livré dans le paquetage.

'**BportMap**' Ce module permet d'émuler le fonctionnement des services **SUN RCP** tels que '**statd**', '**tooltalk**', '**rquota**', '**sadmind**'. L'auteur indique avoir écrit ce module dans l'optique de créer des règles '**snort**' correspondant à des codes d'exploitation en sa possession mais pour lesquels il ne disposait d'aucune machine vulnérable.

'**Honeyd-win**' Ce paquetage correspond au portage de l'outil '**honeyd**' en environnement **WIN32** autorisant ainsi son utilisation sur un système Windows. Ce paquetage est disponible sous forme source nécessitant une compilation sur le système cible – et donc la disponibilité d'un compilateur C - mais aussi sous forme binaire directement exploitable.

'**gmhoney**' Ce module permet d'émuler le fonctionnement du service de messagerie '**smtp**'. Il nécessite l'installation préalable du **JRE** 1.4 (Java Run Time).

'**HoneydGUI**' Cette interface graphique facilite la configuration du service '**honeyd**' ainsi que la génération des fichiers spécifiques. La topologie réseau peut être visualisée et aisément modifiée.

'**honeyweb**' Ecrit en langage 'python', cet utilitaire peut être utilisé de manière autonome ou intégré au service '**honeyd**'. Il permet de simuler le comportement réseau d'un serveur WEB et fonctionne aussi bien en environnement **UNIX** que **WIN32**.

'**gala**' Utilitaire permettant de remonter à la source géographique des attaques, '**gala**' fait partie d'un projet plus vaste visant à pouvoir traiter les journaux issus de divers équipements de surveillance ou de production: '**honeyd**', '**predule IDS**', '**apache**', … La version proposée reste difficilement exploitable. Le projet '**Gala**', initié par Philippe Bourcier, sera maintenu sur le site WEB '**http://sysctl.org/gala/**'

On notera que depuis 31 Mars 2003, le site de **Niels Provost** hébergé sur le site de l'université du **Michigan** n'est plus accessible. Un routage est réalisé sur une page hébergée en hollande où l'on peut lire l'information suivante:

*Due to a new **Michigan law**, the legality of my research or these web pages is currently unclear.*
Felton provides additional information about the resulting restrictions on technology and research.

Il s'agit ici d'un nouvel avatar du DMCA – Digital Millenium Copyright Act – légiféré par l'état du Michigan. Nous conseillons à nos lecteurs d'étudier attentivement les 9 articles de cette loi mise en application le 31 mars 2003 sous la référence '750.540c.amended: Prohibited conduct with regard to telecommunications access device; violation as felony; penalty; amateur radio service; forfeiture; order; definitions.'



Fort heureusement, **Niels Provost** nous propose de continuer à accéder à son site alternatif sous réserve de répondre à trois questions en s'engageant sur l'honneur quand à l'exactitude des réponses fournies:

1. Etes-vous un citoyen des Etats-Unis ?
2. Etes-vous physiquement localisé sur le territoire des Etats-Unis ?
3. Est-il légal dans le pays d'ou vous vous connectez de distribuer du logiciel ou une information cryptographique qui délivre ou informe à propos des procédés cryptographiques ou stéganographiques ?

▪ **Complément d'information**

http://niels.xtdnet.nl/honeyd/index.php
http://www.citi.umich.edu/u/provos/honeyd/ch01-results/
http://www.freedom-to-tinker.com/superdmca.html
http://www.michiganlegislature.org/printDocument.asp?objName=mcl-750-540c-amended&version=txt

ROOTKITS

IDEFENSE – ETAT DE L'ART DES ROOTKITS

▪ **Description**



La société '**iDefense**', très certainement connue de nos lecteurs pour ses alertes de sécurité, a publié en Février dernier une étude fort intéressante portant sur les outils d'attaque pré-packagés dénommés '**rootkit**'.

Avant d'étudier le contenu de cette étude, il peut être utile de donner notre définition du '**rootkit**' et d'en rappeler la genèse:

> *Un 'rootkit' est une collection, organisée et prête à l'emploi, d'utilitaires permettant d'ouvrir, et de conserver, un accès masqué sur un compte unix disposant de privilèges étendus, ceux de 'root' en général.*

Bien que les techniques élémentaires de dissimulation et de masquages utilisées dans les '**rootkits**' aient fait l'objet de multiples articles publiés dés **1986**, le terme '**rootkit**' n'est réellement apparu qu'au milieu des années **90**.

Jusqu'alors, les pirates disposaient de leurs propres boîtes à outils laborieusement assemblées et jalousement défendues. En effet, rares étaient les systèmes d'exploitation accessibles à tout un chacun en dehors des systèmes de type **BSD** et dérivés - **SunOS** par exemple - dont les sources étaient assez facilement disponibles dans le milieux universitaire. Ainsi, les premiers composants des futurs '**rootkits**' firent leur apparition en environnement **BSD4.x** puis **SunOS**.

Citons à titre d'exemple, les deux articles de fond publiés dans le célèbre magazine '**PHRACK**':

- **Unix Cracking Tips** (*Phrack Vol. 3 / Num. 25 / Art. 5 en date du 17 Mars 1989*) ou comment manipuler le noyaux UNIX afin de détourner, voire d'ajouter, certains appels systèmes en environnement **BSD**.
- **Hidding Out Under UNIX** (*Phrack Vol. 3 / Num. 25 / Art. 6 en date du 25 Mars 1989*) ou comment manipuler le contenu du fichier **/etc/utmp** en environnement **BSD** et **Systeme V** afin de masquer toute trace des connexions console.

Il est possible d'affirmer, avec le recul, que le numéro **25** de **PHRACK Magazine** marque l'apparition (pour ne pas dire "est à l'origine") d'une nouvelle ère en dévoilant des techniques de manipulations performantes, et jusqu'alors totalement confidentielles, auprès d'un large public (pour l'époque).

Il faudra cependant attendre encore cinq ans, et l'article '**The Fingerd Trojan**' (*Phrack Vol. 5 / Num. 46 / Art. 1 en date du 20 Septembre 1994*), pour voir apparaître la technique consistant à modifier - patcher - les sources d'un service, ici '**finger**', dans l'optique de lui adjoindre une porte dérobée.

Tous les éléments sont alors réunis pour favoriser l'éclosion de boîtes à outils prêtes à l'emploi:

- les techniques élémentaires sont désormais connues, les composants logiciels sont développés sous la forme de modules facilement adaptables grâce aux outils **GNU**,
- un réseau de communication dénommé **Internet** ouvert et performant est désormais accessible qui autorise non seulement l'échange de données mais aussi l'ouverture programmable de connexions en temps réel,
- les sources de systèmes d'exploitation 'universitaires' sont accessibles à tous, **SUN** annonce la mise à disposition gracieuse de la version **X86** de son nouveau système **Solaris**, *Linus Torvald* relève le défi de créer un système d'exploitation totalement libre: **LINUX**.

Le résultat ne se fait pas attendre, entre **1995** et **2001**, plus de trente paquetages de type '**rootkit**' sont diffusés et fonctionnels en majorité dans l'environnement **LINUX** mais aussi sous **Solaris** et **FreeBSD**.

En **1996**, un paquetage réunissant toutes les caractéristiques attendues d'un '**rootkit**' est rendu publique. Ce paquetage dénommé '**LRK V3**' - pour **Linux Root Kit** - fera l'objet de trois évolutions successives, la version '**LRK V5**' publiée fin 1999 atteignant un degré de sophistication rarement égalét: 18 utilitaires classiques modifiés - dont **chfn**, **chsh**, **du**, **find**, **ifconfig**, **inetd**, **killall**, **login**, **netstat**, **passwd**, **pidof**, **ps**, **rshd**, **syslogd**, **tcpd** et **top** - et 6 outils spécifiques.

En **1997**, deux articles détaillant une technique de manipulation dynamique des librairies partagées sont publiés dans PHRACK sous les titres évocateurs de '**Shared Library Redirection**' (*Phrack Vol. 7 / Num. 51 / Art. 8 en date du 01 Septembre 1989*) et '**Bypassing Integrity Checking Systems**' (*Phrack Vol. 7 / Num. 25 / Art. 9 en date du 01 Septembre 1989*).

Combiné avec le mécanisme de chargement des modules, présents notamment en environnement **Solaris** et **Linux**, cette technique autorise la création d'un nouveau type de '**rootkit**' plus efficace dans lequel la fonction de



dissimulation est codée au niveau du noyau, et non plus dans chaque utilitaire.

En 1999, un nouvel article de Phrack, '**A *REAL* NT Rootkit, patching the NT Kernel**' (*Phrack Vol. 9 / Num. 55 / Art. 5 en date du 09 Septembre 1999*), détaille la technique permettant de manipuler le noyau du système d'exploitation NT afin d'y installer un '**rootkit**'.

Enfin, à la veille du passage en l'an 2000, l'existence des '**rootkits**' est enfin dévoilée au grand public par un **article** de **Dave Dittrich**, un universitaire collaborant à l'initiative de sécurité mise en place par le **SANS**. Depuis, plusieurs autres paquetages aussi performants que le '**LRK**' ont été diffusés dont notamment '**t0rnKit**' et '**adore**' …

En **mars 2001**, le projet '**HoneyNet**' propose son 13ième défi dont l'objectif est d'analyser '**LuckRoot**', un '**rootkit**' découvert sur un système Linux compromis, puis en Juin 2001, le 16ième défi qui consiste à déchiffrer le code d'un autre '**Rootkit**'. Le lecteur pourra se reporter à nos analyses présentées dans les rapports N°32 et 35 pour en savoir plus.

Avec son étude de 27 pages intitulée '**An overview of Unix RootKits**', la société **iDefense** nous propose un tour d'horizon des différentes techniques mises en œuvre par ce type d'outils d'attaque en détaillant notamment les différents procédés permettant de maintenir un accès sur le système compromis.

Sont ensuite étudiées les trois classes de '**RootKits**' déterminées par le moyen employé pour installer le(s) code(s) actif(s) :

- modification de certains binaires du système,
- centralisation du code dans un module chargé dynamiquement dans le noyau dit 'LKM',
- ou encore dans une librairie dynamique du système.

Enfin, trois 'RootKits' classiques sont analysés en détail en fin d'étude:

- '**Sa**' apparu en 2001 qui exploite une vulnérabilité présente dans la version de l'époque du serveur **WU-Ftp** et remplace de nombreux binaires systèmes,
- '**W00tkit**' l'une des multiples variations du célèbre rootkit '**T0rn**' apparu début 2000 qui s'installe notamment dans la librairie système '**libproc**',
- '**RK**' une adaptation roumaine du célèbre LKM '**adore**'.

Le sommaire de cette très instructive étude est le suivant :

Nous recommandons la lecture de ce document à tout personne soucieuse de comprendre le fonctionnement d'un '**rootkit**' et les risques associés à l'installation de celui-ci sur un quelconque système: système personnel, poste bureautique ou serveur.

▪Complément d'information

http://www.idefense.com/papers.html



INFORMATIONS ET LEGISLATION

LES INFORMATIONS

CRYPTOGRAPHIE

CHALLENGE RSA 160

▪ **Description**

En 1991, la société **RSA Security** lançait à la communauté des cryptanalystes une série de 41 défis intitulés '**RSA Factoring challenge**' dont l'objectif consistait en la factorisation – réduction sous la forme des deux facteurs premiers - de nombres dont la longueur s'échelonnait de 100 à 500 chiffres par pas de 10 chiffres. Par le passé, quatre de ces défis ont été remportés dont **RSA-129**, **RSA-130**, **RSA-140** (terminé le 2/02/1999) et **RSA-155** (terminé le 22/08/1999).

Devant le calme plat qui s'était installé après cette série de défi – 2 ans sans qu'aucun des défis '**RSA Factoring Challenge**' restant n'ait été tenté – la société **RSA Security** annonçait, mi-Mai 2001, la reprise de la série de défis '**RSA Factoring challenge**' sous une nouvelle forme en offrant une dotation allant de $10 000 à $200 000 avec l'ouverture de huit nouveaux défis (Rapport N° 34 – Mai 2001).

Le 1er Avril 2003 (sic), une équipe de l'université de **Bonn** a cependant annoncé être venue à bout de **RSA-160**, l'un des défis restant à résoudre dans la première série. Rappelons qu'à l'époque, le nom du défi exprimait la taille du nombre devant être factorisé en digits (chiffres décimaux), soient **540 bits** dans le cas de ce défi.

Si le défi **RSA-155** (512 bits) n'avait demandé que 7,4 mois calendaires de travail en durée mais 35,7 années équivalentes de puissance de calcul distribuée sur 160 SUN 175/400Mhz, 8 SGI 200Mhz, 120 PII 300/400Mhz, 4 Digital 500Mhz, le défi **RSA-160** (540 bits) n'a nécessité que 17 jours de travail en s'appuyant sur 32 R12000 et 72 stations alpha EV67.

Utilisant la méthode de crible dite '**General Number Field Sieve**' ou '**GNFS**', cette factorisation a bénéficié des remarquables progrès en matière de puissance de calcul disponible constatée depuis la dernière factorisation réussie (1999).

Défi	Date	Taille	Durée
RSA-100	1991	NA	NA
RSA-110	1992	NA	NA
RSA-120	1993	NA	NA
RSA-129	1977	426 bits	32 sem.
RSA-130	1996	428 bits	33 sem.
RSA-140	1999	465 bits	9 sem.
RSA-155	1999	512 bits	30 sem.
RSA-160	2003	540 bits	2 sem.

Les huit défis de la nouvelle série restent à ce jour ouverts à qui souhaite tenter sa chance :

Défi	Prix	Digits	Nombre à factoriser
RSA-576	$ 10 000	174	188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059
RSA-640	$ 20 000	193	3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609
RSA-704	$ 30 000	212	74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359
RSA-768	$ 50 000	232	1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413
RSA-896	$ 75 000	270	412023436986659543855531365332575948179811699844327982845455626433876445565248426198098870423161841879261420247188869492560931776375033421130982397485150944909106910269861031862704114880866970564902903653658867433731720813104105190864254793282601391257624033946373269391
RSA-1024	$100 000	309	135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563
RSA-1536	$150 000	463	1847699703211741474306835620200164403018549338663410171471785774910651696711161249859337684305435744585616061544571794052229717732524660960646946071249623720442022269756756687378427562389508764678440933285157496578843415088475528298186726451339863364931908084671990431874381283363502795470282653297802934916155811881049844908319545009848393775227257052578591944993870073695755688436933812779613089230392569695253261620823676490316036551371447913932347169566988069
RSA-2048	$200 000	617	25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357



▪Complément d'information

http://www.loria.fr/~zimmerma/records/factor.html
http://www.loria.fr/~zimmerma/records/rsa160
http://www.nfsnet.org/faq-nfs.html

WIFI

DCSSI – SECURITE DES RESEAUX WIFI

▪Description

La mission de produire des recommandations relatives à l'utilisation et à l'exploitation des réseaux sans fil avait été confiée à Henri SERRES, Directeur central de la sécurité des systèmes d'information au Secrétariat général de la Défense Nationale, par les ministres de l'industrie et de la recherche.

La **DCSSI** a ainsi élaboré deux documents :

- Une **présentation synthétique** de la sécurité des réseaux utilisant la norme 802.11b (Wi-Fi)
- Un document qui présente une analyse des **différents types de risques** auxquels les réseaux Wi-Fi sont exposés, ainsi qu'une série de **conseils** permettant de mieux contrôler le niveau de sécurité et si possible de réduire les risques.

Le premier document présente en 2 pages les éléments dont il faudra tenir compte lors de l'établissement d'un réseau sans fil:

1. Les risques liés à l'utilisation de cette technologie,
2. La planification et l'organisation du déploiement,
3. La protection physique des matériels et des sites,
4. Les mécanismes de protection: chiffrement et authentification.

Le second document de 9 pages intitulé '**Recommandations: La sécurisation des réseaux sans fil**' aborde dans le détail les différents risques liés à l'utilisation de la technologie dite 'sans fil', et plus précisément, celle des réseaux **IEEE802.11b**.

Sont ainsi exposées les attaques portant sur la disponibilité du réseau, sur l'intégrité et la confidentialité des informations transportées. Au delà de la désormais classique attaque exploitant la vulnérabilité du protocole '**WEP**', voire l'absence de tout mécanisme de protection, la présentation synthétique qui nous est proposée a le mérite de rappeler la simplicité de la mise en place d'attaques en déni de service sur ces réseaux : brouillage sélectif ou non dans la bande utilisée dont nous rappelons qu'elle est partagée, saturation volontaire du point d'accès conduisant celui-ci à rejeter le trafic sans distinction d'aucune sorte.

Nous conseillons la lecture de ces deux documents dont nous avons particulièrement apprécié la forme pédagogique rendant ceux-ci accessibles à tous.

▪Complément d'information

http://www.ssi.gouv.fr/fr/actualites/Rec_WIFI.pdf
http://www.ssi.gouv.fr/fr/actualites/synthwifi.pdf

TENDANCES

ICSA – 8IEME RAPPORT ANNUEL

▪Description



La division '**ICSA Labs**' de la société '**TruSecure**' vient de publier son 8ième rapport annuel intitulé '8th Annual Virus Prevalence Survey' portant sur les tendances observées en matière d'évolution des attaques virales et codes mobiles.

Les résultats de cette étude mettent en évidence deux points clefs sur l'année 2002:

- une nette diminution du taux de croissance des infections hélas considérée par les auteurs du rapport comme n'étant qu'un phénomène transitoire.
- l'absence du grand événement - 'big bang malicious code event' - jusqu'alors observé chaque année par le passé et à l'origine de la majorité des désastres reportés par les sociétés interrogées : **Melissa** en 1999, **LoveLetter** en 2000 et **Nimda** en 2001. En 2002, les 80 désastres mentionnés par les personnes interrogées ont eu pour origine 4 virus sur une période de 9 mois.

Le rapport de 52 pages contient de nombreux tableaux statistiques et graphiques établis sur la base des réponses au questionnaire dont une copie est jointe en fin de rapport. En pratique, 306 réponses ont été considérées comme valables vis à vis des critères établis pour cette étude. L'analyse de ces réponses a permis de dégager 80 cas ayant donné lieu à un désastre au sens des critères technico-économiques établis par l'**ICSA**.

Un premier tableau intéressant extrait du rapport – page 14 - détaille les virus à l'origine des désastres les plus récents:



Nom du virus code mobile	Fréquence dans les réponses	Nombre de machines impliqués
KELZ	17	121 278
NIMDA	20	86 285
YAHA	7	68 265
LOVELETTER	4	33 395
BUGBEAR	13	18 266
BADTRANS	8	13 997
FUNLOVE	4	11 685
SIRCAM	2	7 011
GONER	2	5 474
OPASERV	2	2 091
MTX	1	1 845

Un second tableau tout aussi intéressant –page 24 du rapport - précise le vecteur de transport utilisé par les virus ou codes mobiles depuis 1996:

Vecteur	1996	1997	1998	1999	2000	2001	2002
Attachement messagerie	9	26	32	56	87	83	86
Téléchargement depuis Internet	10	16	9	11	1	13	11
Parcours de sites WEB	0	5	2	3	0	7	4
Distribution de logiciel	0	3	3	0	1	2	0
Disquette ou autre média	71	84	64	27	7	1	0
Autres vecteurs	0	5	1	1	1	2	3
Ne sais pas	15	7	5	9	2	1	1

Ces données confirment l'importance - pour ne pas dire la part prépondérante - de la messagerie électronique dans la distribution et la propagation des virus, le second vecteur semblant être celui du transfert par le biais des services Internet. De notre point de vue, les années à venir devraient faire apparaître un rééquilibrage entre les deux principaux modes de propagation: la messagerie et l'exploitation automatisée de vulnérabilités, ce mode n'étant hélas pas explicitement identifié et pris en compte dans l'étude de l'ICSA.

La table des matières de ce rapport est la suivante:

▪**Complément d'information**

http://www.trusecure.com/download/dispatch/VPS2002.pdf
http://www.trusecure.com/download/dispatch/vps-survey-2001.pdf



NIST - SP800-50v2 / Building an Information Technology Security Awareness ..

▪Description

Le '**NIST**' propose à la relecture la seconde version d'un guide de 74 pages destiné à faciliter la mise en œuvre d'un processus de sensibilisation et de formation à la sécurité des systèmes d'information.

Intitulé '**Building an Information Technology Security Awareness & Training Program**', ce guide est principalement destiné aux instances gouvernementales américaines dans la cadre du programme **FISMA** (Federal Information Security Management) et de la circulaire A-130 émise par l'**OMB** (Office Management and Budget).

Rappelons en effet que la circulaire **A-130** requiert que toute organisation fédérale soit à même d'évaluer le niveau de sécurité de son système d'information et que chaque agence est tenue de prendre toutes les mesures techniques et organisationnelles permettant de maintenir la sécurité à un niveau compatible avec les exigences décrites dans le guide **SP800-53** à venir '**Minimum Security Controls For Federal Information Technology Systems**'.

Dans ce cadre, la mise à disposition d'un guide permettant de structurer la démarche de formation et de sensibilisation absolument indispensable à la bonne mise en œuvre du programme fédéral est une absolue nécessité.

Même s'il a été initialement conçu dans un cadre gouvernemental, ce guide contient de nombreux principes qui pourront être transposés sans grande difficulté dans un contexte privé.

▪Complément d'information

http://csrc.nist.gov/publications/drafts/SP800-50-version2Draft.pdf

NIST – Etat des guides de la serie SP800

▪ Description

La disponibilité de la nouvelle version du document **SP800-50** nous amène à proposer une mise à jour du tableau récapitulatif des publications récentes de la série spéciale '**SP800**':

SP800-26	Security Self-Assessment Guide for Information Technology Systems	[F]	11/2001
SP800-27	Engineering Principles for Information Technology Security	[F]	06/2001
SP800-28	Guidelines on Active Content and Mobile Code	[F]	10/2001
SP800-29	Comparison of Security Reqs for Cryptographic Modules in FIPS 140-1 & 140-2	[F]	10/2001



SP800-30	Underlying Technical Models for Information Technology Security	[F]	01/2002
SP800-31	Intrusion Detection Systems	[F]	11/2001
SP800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure	[F]	02/2001
SP800-33	Underlying Technical Models for Information Technology Security	[F]	12/2001
SP800-34	Contingency Planning Guide for Information Technology Systems	[F]	06/2002
SP800-35	Guide to Selecting IT Security Products	[R]	10/2002
SP800-36	Guide to IT Security Services	[R]	10/2002
SP800-37	Guidelines for the Security C&A of Federal Information Technology Systems	[R]	10/2002
SP800-38	Recommendation for Block Cipher Modes of Operation	[F]	12/2001
SP800-40	Applying Security Patches	[*]	09/2002
SP800-41	Guidelines on Firewalls and Firewall Policy	[F]	01/2002
SP800-42	Guidelines on Network Security testing	[R]	04/2002
SP800-43	System Administration Guidance for Windows2000	[R]	01/2002
SP800-44	Guidelines on Securing Public Web Servers	[*]	09/2002
SP800-45	Guide On Electronic Mail Security	[*]	09/2002
SP800-46	Security for Telecommuting and Broadband Communications	[*]	09/2002
SP800-47	Security Guide for Interconnecting Information Technology Systems	[*]	09/2002
SP800-48	Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices	[R]	07/2002
SP800-50	**Building an Information Technology Security Awareness & Training Program**	[V2]	03/2003
SP800-51	Use of the Common Vulnerabilities and Exposures Vulnerability Naming Scheme	[F]	09/2002
SP800-53	Minimum Security Controls For Federal Information Technology Systems	[D]	
SP800-53a	Techniques & Prodedures for the verification of Security Controls in Fed. ITS	[D]	
SP800-55	Security Metrics Guide for Information Technology Systems	[R]	10/2002
SP800-56	**Recommendation on Key Establishment Schemes**	[D]	01/2003
SP800-57	**Recommendation on Key Management**	[D]	01/2003

[F] Finalisé **[*]** Récemment finalisé
[R] Pour commentaire et relecture **[D]** En cours de développement

- **Complément d'information**

http://csrc.nist.gov/publications/nistpubs/index.html

CONFERENCES

CANSECWEST 2003

- **Description**

CanSecWest/core03

L'édition **2003** de la célèbre conférence '**CanSecWest**' s'est tenue du 9 au 11 Avril à **Vancouver**. Les textes des présentations sont partiellement accessibles sur le site officiel.

A la lecture des présentations, on constatera que plus de la moitié d'entre elles ont déjà été exposées aux conférences '**HIVERCON 2002**' et plus récemment '**BlackHat 2003**' (Rapport N°56 – Mars 2003).

Nous proposons ci-après au lecteur un présentation synthétique des quelques thèmes ayant attiré notre attention parmi les 14 présentations effectuées.

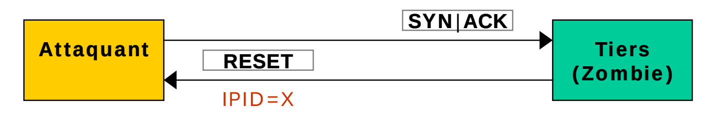
Advanced network reconnaissance techniques **Fyodor**

Fyodor, l'auteur du célèbre outil de sondage '**nmap**' présente le nouveau procédé d'analyse désormais intégré dans la dernière version de son outil. Dénommé '**Idle Scan**', ce procédé permet de détecter la présence d'un service actif sur le système cible sans jamais exposer l'adresse IP du système de l'utilisateur en s'appuyant sur un système tiers.

Nous reprenons ci-dessous le diagramme des échanges présenté par '**Fyodor**'

Etape N°1: **Recherche d'un système tiers appelé 'ZOMBIE'**

Il s'agit ici d'obtenir le numéro de séquence '**IP**' (ou **IPID**) couramment utilisé par le système tiers. Pour cela, un sondage furtif utilisant un paquet '**SYN/ACK**' est engagé. Le système tiers répondra par un paquet '**RESET**' indiquant une erreur dans le séquencement de l'ouverture de la connexion **TCP**. Ce paquet contient le numéro de séquence courant utilisé par le système tiers.



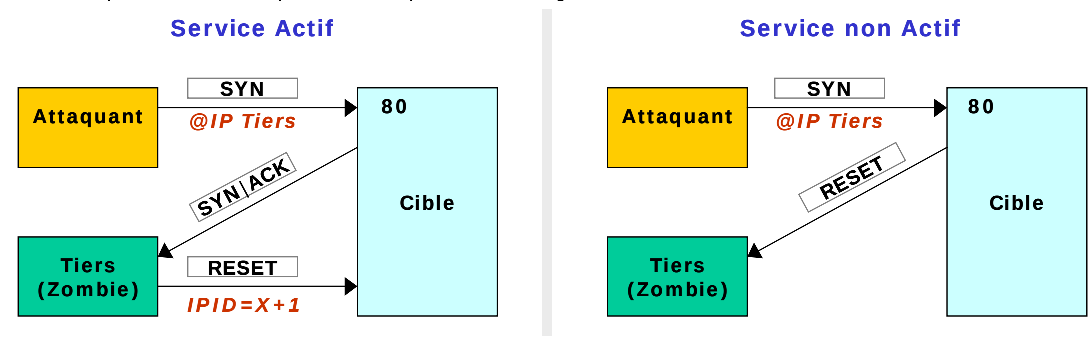
Etape N°2: **Sondage du service cible en usurpant l'adresse du 'Zombie'**



L'attaquant va maintenant tenter d'ouvrir une session vers le service cible en utilisant l'adresse IP du système tiers. Deux possibilités doivent alors être considérées:

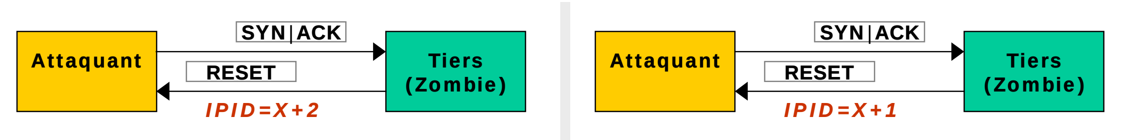
- **Le service cible est actif**: le système tiers reçoit une réponse de la part du système cible à une requête qu'il n'a jamais initié. Il retransmet en conséquence un paquet **RESET** à l'attention du système cible en incrémentant le numéro de séquence **IP**.

- Le service cible est inactif: le système tiers reçoit un paquet **RESET** de la part du système cible. Le numéro de séquence **IP** n'est pas modifié par cet échange.



Etape N°3: Analyse de l'état du service cible

L'attaquant peut maintenant déterminer l'état du service cible en analysant la valeur actuelle du numéro de séquence **IP** maintenu par le système tiers par un test identique à celui de la première étape. Le numéro de séquence sera automatiquement incrémenté à la suite de cet échange. L'attaquant peut alors tirer la conclusion suivante: une différence de deux unités entre les numéros de séquence final et initial indique qu'un échange a eu lieu entre la cible et le système tiers et qu'en conséquence, le service cible est actif. Bien entendu, l'enchaînement des opérations devra être optimal et le système tiers 'peu actif' pour garantir que l'évolution du numéro de séquence ne soit pas le fait d'une session 'parasite' licite ou non.



Cette technique, fort astucieuse, permet de berner l'exploitant du système cible en amenant éventuellement celui-ci à engager une procédure envers un tiers totalement '**innocent**'. Quelques exemples d'alertes remontées par **BlackIce Defender** sont présentés dont le plus intéressant met en évidence une tentative d'attaque de la part du **CERT-CC** dont le serveur WEB a été choisi comme '**zombie**'.

Les RSSI et exploitants devront désormais prendre garde à ne pas engager la responsabilité d'un tiers sur la seule base de l'adresse source ou du nom de domaine remonté par les équipements **IDS**.

IDS data correlation — Jed Haile

Cette présentation effectuée par **Jed Haile** de la société **Nitro Data System** porte sur l'utilisation de '**Argus**' (Rapport N°42 – Janvier 2002), un outil d'audit des transactions **IP** pour améliorer la qualité de l'analyse des intrusions, ou plus exactement, pour extraire les évènements réellement pertinents.

On notera l'annonce de la prochaine disponibilité d'une version commerciale éditée par la société **Qosient** d'**Argus** jusqu'alors accessible gratuitement car résultant d'un contrat passé entre le département américain de la défense et l'université de Carnegie-Mellon.

Advances in OpenBSD — Theo DeRaadt

La présentation effectuée par **Theo DeRaadt**, l'unique responsable de l'évolution du système '**OpenBSD**', propose un bilan de l'utilisation des fonds – 2.3 million de dollars – attribués par le **DARPA** dans le cadre du financement de projets ayant trait à la sécurité. Ces fonds ont ainsi permis d'employer 6 développeurs à plein temps, d'acheter du matériel, d'organiser une session de codage d'une semaine mais aussi de financer l'audit du projet **OpenSSL**.

Les nouveaux développements ont principalement porté sur:

- La réduction du nombre d'exécutables dits '**SUID**', c'est à dire s'exécutant avec les privilèges du propriétaire, '**root**' en général. Ce travail conséquent de réorganisation des groupes, des utilisateurs mais aussi de modification du code a permis de produire une distribution ne contenant plus que 8 binaires '**SUID**' au lieu des 40 binaires '**SUID**' précédemment livrés: '**chfn**', '**login**', '**passwd**', '**rsh**', '**su**', '**sudo**', '**lockspool**', '**authpf**'. Dans la même logique, un effort visant à diminuer le nombre d'utilitaires '**SGID**' – s'exécutant avec les privilèges du groupe - a aussi été engagé.
- Le renforcement du principe élémentaire de sécurité dit de 'séparation des privilèges'. Le procédé utilisé consiste à regrouper les opérations à risque dans un processus s'exécutant dans un contexte restreint – 'jail process' dans le jargon – les autres opérations étant gérées par un second processus pouvant s'exécuter avec des privilèges élevés. Les deux processus communiquent par l'intermédiaire d'un canal de type 'socket'. A ce jour, les services **SSH** ('sshd'), **X11** (et le lanceur 'xdm') et l'utilitaire '**xconsole**' ont subit cette modification, les services **WEB** ('httpd'), **FTP** ('ftpd'), **ISAKMP** ('isakmpd') étant en cours d'étude.



- La révocation des privilèges conformément au second principe de sécurité dit 'du moindre privilège'. A cette fin, de nombreux utilitaires ont été modifiés pour relâcher l'identifiant d'utilisateur (**UID**) et de groupe (**GID**) après avoir effectué un changement du point de référence par modification de la racine de l'arborescence vue par le processus (opération dénommée '**chroot**'). Ont ainsi fait l'objet d'une modification les utilitaires '**ping**', '**ping6**', '**traceroute**', '**traceroute6**', '**write**', '**rwalld**', '**pppd**', '**spamd**', '**authpf**', '**portmap**', '**rpc.users**', '**rpc.statd**', '**ftpd**', '**named**' et enfin '**httpd**'.
- Le renforcement de la sécurité du processus '**httpd**' chargé de gérer les accès **WEB**. Ce processus s'exécute désormais dans un contexte restreint – 'jail' ou 'prison' – localisé sous '**/var/www**' après que les modules nécessaires aient été chargés. Les chemins d'accès déclarés dans le fichier de configuration sont automatiquement translatés pour refléter le changement de point de référence.
- La mise en place de 5 mécanismes destinés à réduire les risques et possibilités d'exploitation d'un débordement de buffer:
  1. Positionnement d'un bloc de taille aléatoire en tête de la pile du processus conduisant à rendre imprédictibles les adresses et les positions mémoires – normalement fixes - utilisées par les codes d'exploitation.
  2. Renforcement du contrôle de la cohérence des structures mémoires par la mise en place aléatoire de témoins – appelés **canaris** dans le jargon – vérifiés en sortie de fonction mais aussi par un réarrangement de la structure de la pile.
  3. Déplacement des chaînes, pointeurs et références constantes dans un segment dédié '**.rodata**' accessible en lecture seule.
  4. Utilisation des capacités de gestion des accès à la mémoire offertes par certaines implémentations de l'unité de gestion de la mémoire ou **MMU** (Memory Management Unit'). En pratique, seuls les processeurs '**sparc**', '**sparc64**', '**alpha**', '**hppa**' autorisent une gestion efficace de la mémoire. Les processeurs '**m68k**', '**vax**' et '**mips**' ne disposent hélas pas des fonctions nécessaires et les processeurs '**Ix86**' et '**powerpc**' nécessitent des manipulations complexes et non satisfaisantes pour arriver au résultat attendu.
  5. Renforcement du positionnement des drapeaux de gestion des accès à la mémoire '**PROT_WRITE**' et '**PROT-EXEC**' de manière à assurer qu'un segment autorisé à l'exécution ne le soit pas à l'écriture.
- L'amélioration et l'extension des fonctionnalités offertes par le célèbre mécanisme filtrage de paquets '**bpf**' avec l'adjonction de règles 'in line', le contrôle de la bande-passante, …

La version **OpenBSD 3.3** dont la disponibilité est annoncée pour le 1 Mai intégrera la majorité de ces évolutions. On notera par ailleurs le discret appel au peuple en matière de contribution financière, le financement apporté par le **DARPA** arrivant sous peu à échéance.

Advances in ELF binary runtime encryption — N.Metha & S.Clowes

La protection des exécutables par chiffrement de tout ou partie de l'image **ELF** du binaire est un procédé ayant vu le jour en environnement **UNIX** en 2001 avec le développement par le groupe '**TESO**' de '**BurnEye**'. Remarquablement conçu et n'ayant fait l'objet d'aucune documentation publique, cet utilitaire a donné du fil à retordre aux analystes ayant eu à étudier le code d'exploitation '**OpenSSL**' dit '**X2**'. Le principe de base employé par de tels outils consiste à chiffrer certains segments de code mais aussi à manipuler les structures fondamentales de l'image binaire dans l'optique de la rendre invalide bien qu'exécutable. La routine de déchiffrement est généralement intégrée dans l'image binaire constituant ainsi son talon d'Achille.

Ce type de procédé est généralement employé – notamment par les auteurs de virus, de codes mobiles et de codes d'exploitation - pour complexifier la rétro-analyse d'un code binaire, voire pour restreindre son utilisation aux seuls groupes d'initiés possédant les clefs d'activation. Pour mémoire, rappelons que les premiers virus intégrant une protection par chiffrement et mutation du code sont apparus dans les années 90 en environnement MSDOS.

Intitulée '**Advances in ELF binary runtime encryption**', la présentation effectuée par **Shaun Clowes** et **Neel Metha** nous propose d'étudier les fonctionnalités attendues d'un mécanisme de protection assurant le déchiffrement au fil de l'eau dont notamment :

- Ralentir l'analyse en rendant celle-ci éventuellement trop coûteuse pour le gain espéré,
- Résister aux techniques classiques d'analyse dynamique consistant à tracer le chemin d'exécution, ou statique par désassemblage du code et/ou analyse des chaînes de caractères,

Plusieurs techniques peuvent être combinées pour atteindre ces objectifs :

- Techniques offensives visant par exemple à activer un mécanisme de défense en cas de tentative de manipulation du programme
- Techniques défensives pouvant consister à rendre inintelligible la structure originale du programme en chiffrant plusieurs fois celui-ci avec des variations aléatoires.

L'attaquant devra alors non seulement déchiffrer chaque niveau de protection positionné à la manière d'une pelure d'oignon mais aussi faire 'sauter' chacune des protections actives dissimulées dans les différents niveaux.

Ces techniques ont été mises en œuvre dans l'utilitaire de protection '**Shiva v0.95**' qui implémente trois niveaux imbriqués de protection:

Niveau 3: Chiffrement particulier

Les sections du code original sont chiffrées sous la forme de blocs réordonnancés, un seul bloc étant présent déchiffré en mémoire à un instant donné.

Niveau 2: Chiffrement général

L'ensemble des blocs précédemment chiffrés indépendamment est de nouveau chiffré à l'aide de l'algorithme '**AES**' en ajoutant un bloc de code assurant la gestion des clefs d'accès.



Niveau 1: **Brouillage ou 'obfuscation'**

Les données du niveau précédent sont simplement brouillées dans l'optique de limiter les résultats d'une analyse statique: recherche de chaînes de caractères spécifiques, de section de code, ….

Les auteurs annoncent qu'ils fourniront les sources de '**Shiva**' d'ici 3 mois en espérant que d'ici là quelqu'un aura réussi à développer une méthode d'attaque générique sur la seule base des éléments fournis: l'outil sous forme binaire et les principes exposés durant la présentation.

▪ **Complément d'information**

http://www.cansecwest.com/resources.cgi

LA LEGISLATION

CYBERCIMINALITE

G8 – PROTECTION DES INFRASTRUCTURES VITALES

▪ **Description**

La première réunion multilatérale consacrée à la protection des infrastructures vitales a eu lieu à Paris du 24 au 26 mars 2003 au Centre de conférences internationales Kléber. Co-parrainée par la France et les Etats-Unis, elle a rassemblé des experts de très haut niveau, membres du G8, ainsi que de grands opérateurs du domaine concerné (pour la France, **France Telecom**).

Le Secrétariat général de la défense nationale organise cette conférence en liaison étroite avec la délégation des Etats-Unis et le sous groupe cyber-criminalité du groupe du G8 chargé des questions de criminalité, dit "groupe de Lyon".

Ils ont eu pour tâche de définir des principes communs de protection des infrastructures vitales de communication. Les recommandations issues de cette conférence seront transmises aux Ministres de la Justice et de l'Intérieur des membres du G8, pour leur réunion de mai 2003.

▪ **Complément d'information**

http://www.ssi.gouv.fr/fr/actualites/index.html

http://www.ssi.gouv.fr/fr/actualites/G8-infra_vitales.html

http://www.g8.fr/evian/francais/navigation/actualites/conference_sur_la_protection_des_infrastructures_vitales_-_g8.html

NORMALISATION

AFNOR / SSI – NOUVELLES ORIENTATIONS DE L'ETAT EN SECURITE DES SI

▪ **Description**

Le jeudi 27 mars, l'**AFNOR** – Association Française de Normalisation – et la **DCSSI** ont organisé une journée ayant pour thème la politique de l'état en matière de sécurité des systèmes d'information et plus particulièrement en ce qui concerne la normalisation. Nous reproduisons ci-dessous, l'introduction proposée par **Henri Serres**, le Directeur de la sécurité des système d'information.

> *Le développement de l'administration électronique et l'accroissement des menaces potentielles sur les réseaux rendent plus nécessaire que jamais la sécurisation des systèmes d'information qui assurent le bon fonctionnement de l'appareil d'Etat.*
>
> *Au cours de l'année 2002, la Commission Interministérielle pour la Sécurité des Systèmes d'Information (**CISSI**) a entrepris de résoudre certaines difficultés auxquelles elle se trouvait confrontée : manque de produits de sécurité qualifiés, faible implication des industriels français, voire européens, dans l'élaboration de tels outils, flou dans les partages de responsabilité entre les différents acteurs, insuffisance de gestion d'ensemble des questions de sécurité dans le développement et l'exploitation des systèmes d'information.*
>
> *Ce travail a conduit à proposer une série d'orientations nouvelles dans les actions à mener et les relations à développer entre les différents acteurs (organisme régulateur, fonctionnaires de sécurité, maîtres d'ouvrages, industriels). Il est apparu aussi indispensable d'améliorer la lisibilité du cadre juridique dans lequel s'inscrit le travail de sécurisation des systèmes d'information de l'appareil d'Etat. Ces orientations ont été récemment approuvées par le Cabinet du Premier ministre.*
>
> *Un point fort de ces nouvelles orientations concerne le développement industriel, au plan national et européen, d'une gamme de produits de sécurité aptes à renforcer la confiance dans les échanges des administrations entre elles et avec les administrés (normes techniques, procédures d'évaluation et certification, politique d'achat, etc.). L'établissement de normes homologuées sous pilotage de l'**AFNOR** représente à cet égard un facteur important de progrès.*

Le lecteur trouvera le programme et le texte des différentes interventions sur le site de la **DCSSI** :



- Allocution d'ouverture
- Programme de travail 2002-2003 pour la commission de normalisation 'Sécurité des Système d'Information'
- Présentation des nouvelles orientations en matière de SSI
- Le document 'Mise à jour des orientations de la doctrine en matière de sécurité des systèmes d'information'
- La présentation des contributions au développement de la normalisation au plan national,
- Un panorama de l'avancement des travaux normatifs en matière de SSI et nouveaux thèmes de prospection,
- Une étude des travaux normatifs en matière de critères d'évaluation de SSI,
- Et les témoignages d'un industriel – **Michelin** – et d'un opérateur – **La Poste** – sur la qualité de la confiance et les preuves électroniques.

Nous recommandons tout particulièrement la lecture de la présentation des nouvelles orientations en matière de SSI et du document de référence '**Mise à jour des orientations de la doctrine en matière de sécurité des systèmes d'information**', ces deux documents étant présentés par la **DCSSI**. On retiendra plus particulièrement les trois orientations fondamentales retenues pour mise en application courant 2003:

1. **Vis-à-vis de tous :**
   Mise au point d'une réglementation plus cohérente, lisible et réaliste prenant en compte la dimension européenne,
2. **Vis-à-vis des responsables et utilisateurs de SI dans l'Etat :**
   Développement d'une culture et de bonnes pratiques en SSI,
3. **Vis-à-vis des fournisseurs :**
   Mise en place de conditions permettant l'élaboration d'une gamme diversifiée de produits et de prestations de sécurité dûment qualifiées.

L'annonce d'une prise de position officielle sur le thème de la normalisation - considéré comme stratégique au moins du point de vue économique mais hélas actuellement largement dominé par la Grande-Bretagne - permet d'envisager pouvoir disposer sous peu de standards et de méthodologies adaptées aux nouvelles orientations et s'intégrant dans le cadre des schémas **ISO 17799**, **BS7799**-part 2 dit **ISMS** mais aussi des critères communs.

- **Complément d'information**

http://www.ssi.gouv.fr/fr/actualites/afnor-dcssi-270303/270303.html

http://www.commoncriteria.org/cc/cc.html



LOGICIELS LIBRES

LES SERVICES DE BASE

Les dernières versions des services de base sont rappelées dans les tableaux suivants. Nous conseillons d'assurer rapidement la mise à jour de ces versions, après qualification préalable sur une plate-forme dédiée.

RESEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.2.2	03/03/03	http://www.isc.org/products/BIND
		8.3.4	16/11/02	
DHCP	Serveur d'adresse	3.0p2	15/01/03	http://www.isc.org/products/DHCP/dhcp-v3.html
NTP4	Serveur de temps	4.1.1c-rc2	26/04/03	http://www.ntp.org/downloads.html
WU-FTP	Serveur de fichiers	2.6.2	29/11/01	http://www.wu-ftpd.org

MESSAGERIE

Nom	Fonction	Ver.	Date	Source
IMAP4	Relevé courrier	2002c1	18/04/03	ftp://ftp.cac.washington.edu/imap/
POP3	Relevé courrier	4.0.5	13/03/03	ftp://ftp.qualcomm.com/eudora/servers/unix/popper/
SENDMAIL	Serveur de courrier	8.12.9	30/03/03	ftp://ftp.sendmail.org/pub/sendmail/RELEASE_NOTES

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.27	03/10/02	http://httpd.apache.org/dist
		2.0.45	30/03/03	
ModSSL	API SSL Apache 1.3.27	2.8.14	23/10/02	http://www.modssl.org
MySQL	Base SQL	3.23.56	13/03/03	http://www.mysql.com/doc/N/e/News-3.23.x.html
		4.012	15/03/03	
SQUID	Cache WEB	2.5s2	17/03/03	http://www.squid-cache.org

AUTRE

Nom	Fonction	Ver.	Date	Source
INN	Gestion des news	2.3.5	31/12/02	http://www.isc.org/products/INN
MAJORDOMO	Gestion des listes	1.94.5	15/01/00	http://www.greatcircle.com/majordomo
OpenCA	Gestion de certificats	0.9.1.1	28/02/03	http://www.openca.org/openca/download-releases.shtml
OpenLDAP	Gestion de l'annuaire	2.1.17	04/04/03	ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/

LES OUTILS

Une liste, non exhaustive, des produits et logiciels de sécurité du domaine public est proposée dans les tableaux suivants.

LANGAGES

Nom	Fonction	Ver.	Date	Source
SPLINT	Analyse de code	3.0.1.6	18/02/02	http://lclint.cs.virginia.edu
Perl	Scripting	5.8.0	12/08/02	http://www.cpan.org/src/index.html
PHP	WEB Dynamique	4.3.1	17/02/03	http://www.php.net/downloads.php

ANALYSE RESEAU

Nom	Fonction	Ver.	Date	Source
Big Brother	Visualisateur snmp	1.9c	15/05/02	http://bb4.com/
Dsniff	Boite à outils	2.3	17/12/00	http://www.monkey.org/~dugsong/dsniff
EtterCap	Analyse & Modification	0.6.9	27/01/03	http://ettercap.sourceforge.net/index.php?s=history
Ethereal	Analyse multiprotocole	0.9.11	10/03/03	http://www.ethereal.com
IP Traf	Statistiques IP	2.7.0	19/05/02	http://cebu.mozcom.com/riker/iptraf/
Nstreams	Générateur de règles	1.0.3	06/08/02	http://www.hsc.fr/ressources/outils/nstreams/download/
SamSpade	Boite à outils	1.14	10/12/99	http://www.samspade.org/ssw/
TcpDump	Analyse multiprotocole	3.7.2	27/02/02	http://www.tcpdump.org/
Libpcap	Acquisition Trame	0.7.2	27/02/02	http://www.tcpdump.org/
TcpFlow	Collecte données	0.20	26/02/01	http://www.circlemud.org/~jelson/software/tcpflow/
TcpShow	Collecte données	1.81	21/03/00	http://ftp7.usa.openbsd.org/pub/tools/unix/sysutils/tcpshow
WinPCap	Acquisition Trame	3.0	10/04/03	http://winpcap.polito.it/news.htm



ANALYSE DE JOURNAUX

Nom	Fonction	Ver.	Date	Source
Analog	Journaux serveur http	5.32	23/03/03	http://www.analog.cx
Autobuse	Analyse syslog	1.13	31/01/00	http://www.picante.com/~gtaylor/autobuse
SnortSnarf	Analyse Snort	021111	02/11/02	http://www.silicondefense.com/software/snortsnarf/
WebAlizer	Journaux serveur http	2.01-10	24/04/02	http://www.mrunix.net/webalizer/download.html

ANALYSE DE SECURITE

Nom	Fonction	Ver.	Date	Source
FIRE	Boite à outils	0.3.5b	29/11/02	http://biatchux.dmzs.com/
curl	Analyse http et https	7.10.4	02/04/03	http://curl.haxx.se/
Nessus	Vulnérabilité réseau	2.0.4	17/04/03	http://www.nessus.org
Nmap	Vulnérabilité réseau	3.27	28/04/03	http://www.insecure.org/nmap/nmap_download.html
Pandora	Vulnérabilité Netware	4.0b2.1	12/02/99	http://www.packetfactory.net/projects/pandora/
Saint	Vulnérabilité réseau	4.2.4	25/04/03	http://www.saintcorporation.com/updates.html
Sara	Vulnérabilité réseau	4.1.4c	14/03/03	http://www.www-arc.com/sara/downloads/
Tara (tiger)	Vulnérabilité système	3.0.3	15/08/02	http://www-arc.com/tara
Tiger	Vulnérabilité système	2.2.4p1	19/07/99	ftp://net.tamu.edu/pub/security/TAMU/tiger
Trinux	Boite à outils	0.81pre0	07/11/01	http://sourceforge.net/projects/trinux/
Whisker	Requêtes HTTP	2.1	29/11/02	http://www.wiretrip.net/rfp/p/doc.asp?id=21
	LibWhisker	1.6	29/11/02	

CONFIDENTIALITE

Nom	Fonction	Ver.	Date	Source
OpenPGP	Signature/Chiffrement			http://www.openpgp.org
GPG	Signature/Chiffrement	1.2.1	25/10/02	http://www.gnupg.org

CONTROLE D'ACCES

Nom	Fonction	Ver.	Date	Source
TCP Wrapper	Accès services TCP	7.6		ftp://ftp.cert.org/pub/tools/tcp_wrappers
Xinetd	Inetd amélioré	2.3.11	15/04/03	http://synack.net/xinetd/

CONTROLE D'INTEGRITE

Nom	Fonction	Ver.	Date	Source
Tripwire	Intégrité LINUX	2.3.47	15/08/00	http://www.tripwire.org/downloads/index.php
ChkRootKit	Compromission UNIX	0.40	03/04/03	http://www.chkrootkit.org/

DETECTION D'INTRUSION

Nom	Fonction	Ver.	Date	Source
Deception TK	Pot de miel	19990818	18/08/99	http://all.net/dtk/index.html
LLNL NID	IDS Réseau	2.6	10/10/02	http://ciac.llnl.gov/cstc/nid/nid.html
Snort	IDS Réseau	2.0.0	14/04/03	http://www.snort.org/dl/
Shadow	IDS Réseau	1.7	21/09/01	http://www.nswc.navy.mil/ISSEC/CID/

GENERATEURS DE TEST

Nom	Fonction	Ver.	Date	Source
Elza	Requêtes HTTP	1.4.5	01/04/00	http://www.stoev.org/elza/project-news.html
FireWalk	Analyse filtres	5.0	20/10/02	http://www.packetfactory.net/firewalk
IPSend	Paquets IP	2.1a	19/09/97	ftp://coombs.anu.edu.au/pub/net/misc
IDSWakeUp	Détection d'intrusion	1.0	13/10/00	http://www.hsc.fr/ressources/outils/idswakeup/download/
UdpProbe	Paquets UDP	1.2	13/02/96	http://sites.inka.de/sites/bigred/sw/udpprobe.txt

PARE-FEUX

Nom	Fonction	Ver.	Date	Source
DrawBridge	PareFeu FreeBsd	3.1	19/04/00	http://drawbridge.tamu.edu
IpFilter	Filtre datagramme	3.4.31	07/12/02	http://coombs.anu.edu.au/ipfilter/ip-filter.html

TUNNELS

Nom	Fonction	Ver.	Date	Source
CIPE	Pile Crypto IP (CIPE)	1.5.4	29/06/01	http://sites.inka.de/sites/bigred/devel/cipe.html
FreeSwan	Pile IPSec	2.00	28/04/03	http://www.freeswan.org
http-tunnel	Encapsulation http	3.0.5	06/12/00	http://www.nocrew.org/software/httptunnel.html
OpenSSL	Pile SSL	0.9.7b	10/04/03	http://www.openssl.org/
OpenSSH	Pile SSH 1 et 2	3.6.1	01/04/03	http://www.openssh.com/
Stunnel	Proxy https	4.04	12/01/03	http://www.stunnel.org
TeraTerm Pro	Terminal SSH2	3.1.3	08/10/02	http://www.ayera.com/teraterm/
Zebedee	Tunnel TCP/UDP	2.4.1	29/05/02	http://www.winton.org.uk/zebedee/



NORMES ET STANDARDS

LES PUBLICATIONS DE L'IETF

LES RFC

Du **22/03/2003** au **25/04/2003**, **39 RFC** ont été publiés dont x RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SECURITE

Thème	Num	Date	Etat	Titre
AVRIL	3514	04/03	Inf	The Security Flag in the IPv4 Header
BENCH	3511	04/03	Inf	Benchmarking Methodology for Firewall Performance

RFC TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Num	Date	Etat	Titre
COPS	3483	03/03	Inf	Framework for Policy Usage Feedback for Common Open Policy Service with Policy Provisioning
ECML	3505	03/03	Inf	Electronic Commerce Modeling Language (ECML): Version 2 Requirements
NAT	3519	04/03	Pst	Mobile IP Traversal of Network Address Translation (NAT) Devices
SIP	3520	04/03	Pst	Session Authorization Policy Element
VTS	3506	03/03	Inf	Requirements and Design for Voucher Trading System (VTS)

AUTRES RFC

Thème	Num	Date	Etat	Titre
H323	3508	04/03	Inf	H.323 Uniform Resource Locator (URL) Scheme Registration
ICAP	3507	04/03	Inf	Internet Content Adaptation Protocol (ICAP)
IEPRER	3523	04/03	Inf	Internet Emergency Preparedness (IEPREP) Telephony Topology Terminology
IMAP	3516	04/03	Pst	IMAP4 Binary Content Extension
IPP	3510	04/03	Pst	Internet Printing Protocol/1.1: IPP URL Scheme
IPV6	3513	04/03	Pst	Internet Protocol Version 6 (IPv6) Addressing Architecture
MPLS	3474	03/03	Inf	Documentation of IANA assignments for GMPLS Resource Reservation Protocol .. ASON
	3475	03/03	Inf	Documentation of IANA assignments for Constraint-Based LSP setup using LDP .. ASON
	3476	03/03	Inf	Documentation of IANA Assignments for LDP, RSVP, and RSVP-TE ext. for Optical UNI Signaling
OSPF	3509	04/03	Inf	Alternative Implementations of OSPF Area Border Routers
PPP	3518	04/03	Pst	Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP)
SIP	3515	04/03	Pst	The Session Initiation Protocol (SIP) Refer Method
SIP	3521	04/03	Inf	Framework for Session Set-up with Media Authorization
SNMP	3512	04/03	Inf	Configuring Networks and Devices with Simple Network Management Protocol (SNMP)
TCP	3517	04/03	Pst	A Conservative Selective Acknowledgment (SACK)-based Loss Recovery Algorithm for TCP

LES DRAFTS

Du **22/03/2003**au **25/04/2003**, 297 drafts ont été publiés: **199** drafts mis à jour, **98** nouveaux drafts, dont **16** drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
DHCP	draft-ietf-dhc-relay-agent-auth-00	21/04	The Authentication Suboption for the DHCP Relay Agent Option
EAP	draft-boursetty-eap-cst-00	03/04	EAP client-side transport
IPSEC	draft-ietf-ipsec-flowmon-mib-tc-00	02/04	IPsec Flow Monitoring MIB Textual Conventions
	draft-ietf-ipsec-dhcp-over-ike-00	15/04	DHCP over IKE
	draft-ietf-ipsec-dhcp-over-ike-dhcpd-00	15/04	Using DHCP server/client backend for DHCP over IKE
	draft-ietf-ipsec-dhcp-over-ike-radius-00	15/04	Using RADIUS backend for DHCP over IKE
	draft-ietf-ipseckey-rr-00	31/03	A method for storing IPsec keying material in DNS
	draft-hwang-ipsec-spiping-00	21/03	SPI-Based health checking mechanism for IPSEC
INTERCEP	draft-baker-slem-architecture-00	31/03	Cisco Support for Lawful Intercept In IP Networks
	draft-baker-slem-mib-00	31/03	Cisco Lawful Intercept Control MIB
MANDATE	draft-bellovin-mandate-keymgmt-00	09/04	Guidelines for Mandating Automated Key Management
MOBILEIP	draft-nikander-mobileip-v6-ro-sec-00	07/04	Mobile IP V6 Route Optimization Security Design Background
	draft-perkins-mobileip-precfg-kbm-00	15/04	Preconfigured Binding Management Keys for Mobile IPv6
MSEC	draft-ietf-msec-arch-00	25/03	The Multicast Security (MSEC) Architecture



PANA	draft-ietf-pana-pana-00	03/04	Protocol for Carrying Authentication for Network Access (PANA)
SSH	draft-ietf-secsh-newmodes-00	24/03	SSH Transport Layer Encryption Modes

MISE A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
AAA	draft-irtf-aaaarch-handoff-01	24/04	Experimental Handoff Extension to RADIUS
AUTH	draft-murray-auth-ftp-ssl-11	27/03	Securing FTP with TLS
DNS	draft-ietf-dnsext-dnssec-records-03	24/03	Resource Records for DNS Security Extensions
DNS	draft-danisch-dns-rr-smtp-01	15/04	A DNS RR for simple SMTP sender authentication
HEALTH	draft-marshall-security-audit-03	14/04	Security Audit and Access Accountability Message Data Definitions
IKE	draft-dupont-ikev2-addrmgmt-02	07/04	Address Management for IKE version 2
IPSEC	draft-ietf-ipsec-esp-v3-05	08/04	IP Encapsulating Security Payload (ESP)
	draft-ietf-ipsec-monitor-mib-06	15/04	IPSec Monitoring MIB
	draft-ietf-ipsec-isakmp-di-mon-mib-05	15/04	ISAKMP DOI-Independent Monitoring MIB
	draft-ietf-ipsec-ike-monitor-mib-04	15/04	Internet Key Exchange (IKE) Monitoring MIB
	draft-ietf-ipsec-sctp-06	08/04	On the Use of SCTP with IPsec
	draft-ietf-ipsec-ikev2-07	22/04	Internet Key Exchange (IKEv2) Protocol
	draft-ietf-ipsec-ciph-aes-xcbc-mac-04	28/03	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
	draft-ietf-ipsec-rfc2402bis-03	08/04	IP Authentication Header
	draft-ietf-ipsec-esn-addendum-01	10/04	Extended Sequence Number Addendum to IPsec DOI for ISAKMP
	draft-ietf-msec-mesp-01	21/03	MESP: A Multicast Framework for the IPsec ESP
	draft-touch-ipsec-vpn-05	15/04	Use of IPsec Transport Mode for Dynamic Routing
IPV6	draft-ietf-send-psreq-03	14/04	IPv6 Neighbor Discovery trust models and threats
IMAP	draft-ietf-imapext-sort-12	24/03	IMAP - SORT AND THREAD EXTENSION
INCH	draft-ietf-inch-iodef-01	01/04	The IDEF Data Model & XML Implementation DTD
ISIS	draft-ietf-isis-hmac-04	23/04	IS-IS Cryptographic Authentication
KRB	draft-ietf-krb-wg-crypto-04	04/04	Encryption and Checksum Specifications for Kerberos 5
LDAP	draft-weltman-ldapv3-proxy-12	23/04	LDAP Proxied Authentication Control
MOBILEIP	draft-ietf-mobileip-mipv6-ha-ipsec-04	24/03	IPsec to protect mobile IPv6 Sig between mobile nodes & home ag
	draft-ietf-mobileip-vpn-problem-solution-01	10/04	Mobile IPv4 Traversal Across IPsec-based VPN Gateways
PANA	draft-ietf-pana-requirements-05	22/04	PANA Requirements and Terminology
	draft-ietf-pana-threats-eval-03	14/04	PANA Threat Analysis and security requirements
PKIX	draft-ietf-pkix-rfc2510bis-08	15/04	Internet X.509 PKI Certificate Management Protocols
	draft-ietf-pkix-rfc2511bis-06	15/04	Internet X.509 PKI Certificate Request Message Format (CRMF)
	draft-ietf-pkix-proxy-05	17/04	Internet X.509 PKI Proxy Certificate Profile
	draft-ietf-pkix-certstore-http-05	24/03	Internet X.509 PKI Certificate Store Access via HTTP
	draft-ietf-pkix-acpolicies-extn-03	07/04	Attribute Certificate Policies extension
RADIUS	draft-congdon-radius-8021x-29	18/04	IEEE 802.1X RADIUS Usage Guidelines
	draft-chiba-radius-dynamic-authorization-18	23/04	Dynamic Authorization Extensions to RADIUS
	draft-aboba-radius-rfc2869bis-20	23/04	RADIUS Support For Extensible Authentication Protocol (EAP)
	draft-aboba-radius-iana-07	24/04	IANA Considerations for RADIUS
SACRED	draft-ietf-sacred-protocol-bss-07	10/04	Securely Available Credentials Protocol
SIGTRAN	draft-ietf-sigtran-security-02	03/04	Security Considerations for SIGTRAN Protocols
SMIME	draft-ietf-smime-hmac-key-wrap-02	21/03	Wrapping an HMAC key with a Triple-DES Key or an AES Key
	draft-ietf-smime-camellia-03	22/04	Use of the Camellia Encryption Algorithm in CMS
SSH	draft-ietf-secsh-fingerprint-01	28/03	SSH Fingerprint Format
	draft-ietf-secsh-dns-04	02/04	Using DNS to securely publish SSH key fingerprints
SYSLOG	draft-ietf-syslog-sign-10	07/04	Syslog-Sign Protocol
TLS	draft-ietf-tls-openpgp-keys-03	02/04	Using OpenPGP keys for TLS authentication
	draft-ietf-tls-rfc2246-bis-04	23/04	The TLS Protocol Version 1.1
WILSON	draft-blake-wilson-xmldsig-ecdsa-05	04/04	ECDSA with XML-Signature Syntax
XMPP	draft-ietf-xmpp-e2e-02	22/04	End-to-End Object Encryption in XMPP

DRAFTS TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Nom du Draft	Date	Titre
AAA	draft-le-aaa-diameter-mobileipv6-03	10/04	Diameter Mobile IPv6 Application
BENCH	draft-ietf-bmwg-ospfconv-term-03	26/03	OSPF Benchmarking Terminology and Concepts
	draft-ietf-bmwg-ospfconv-intraarea-04	26/03	Benchmarking Methodology for Basic OSPF Convergence
	draft-ietf-bmwg-ospfconv-applicability-02	26/03	Benchmarking Applicability for Basic OSPF Convergence
BGP	draft-libin-hierarchy-pe-bgp-mpls-vpn-01	21/03	Hierarchy of Provider Edge Device in BGP/MPLS VPN
iSCSI	draft-gilligan-iscsi-fault-tolerance-00	03/04	iSCSI Imp. Guide for Fault Tol. & Load Bal. using Temp. Redirect.
L2TP	draft-ietf-l2tpext-v92-moh-05	26/03	Signalling of Modem-On-Hold status in L2TP
LDAP	draft-ietf-ldapext-ldap-java-api-18	03/04	The Java LDAP Application Program Interface
	draft-weltman-ldapv3-auth-response-09	24/04	LDAP Authorization Identity Request and Response Controls
	draft-legg-ldapext-component-matching-10	02/04	LDAP & X.500 Component Matching Rules
MOBILEIP	draft-ietf-mobileip-vpn-problem-stat-req-02	11/04	Problem Statement: Mobile IPv4 Traversal of VPN Gateways
MPLS	draft-behringer-mpls-vpn-auth-02	10/04	MPLS VPN Import/Export Verification
NAT	draft-ford-natp2p-00	08/04	Network Address Translation and Peer-to-Peer Applications
NGTRANS	draft-ietf-ngtrans-isatap-13	04/04	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
PKIX	draft-ietf-pkix-pr-tsa-04	07/04	Policy Requirements for Time-Stamping Authorities
RAP	draft-ietf-rap-feedback-fr-pib-06	07/04	Framework Policy Information Base for Usage Feedback
RSERP	draft-xie-rserpool-redundancy-model-00	07/04	RSERPOOL Redundancy-model Policy
TRACE	draft-ietf-ccamp-tracereq-01	07/04	Tracing Requirements for Generic Tunnels
TTP	draft-ross-ptp-00	22/04	Telephony Tunneling Protocol (TTP)



TUNNEL	draft-templin-tunnelmtu-00	01/04	Path MTU Support for IPv6-in-IPv4 Tunnels
VPN	draft-rosen-vpn-mcast-05	07/04	Multicast in MPLS/BGP VPNs
	draft-kompella-ppvpn-l2vpn-03	15/04	Layer 2 VPNs Over Tunnels
	draft-marques-ppvpn-rt-constrain-00	04/04	Constrained VPN route distribution
	draft-ietf-ppvpn-gre-ip-2547-02	31/03	Use of PE-PE GRE or IP in RFC2547 VPNs

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
3GPP	draft-ietf-v6ops-3gpp-cases-03	01/04	Transition Scenarios for 3GPP Networks
	draft-ietf-v6ops-3gpp-analysis-03	31/03	Analysis on IPv6 Transition in 3GPP Networks
6BONE	draft-fink-6bone-phaseout-01	18/04	6bone (IPv6 Testing Address Allocation) Phaseout
	draft-ymbk-6bone-arpa-delegation-01	02/04	Delegation of 3.F.F.3.IP6.ARPA
AAA	draft-le-aaa-mipv6-requirements-02	10/04	Mobile IPv6 Authentication, Authorization, and Accounting Reqs
ADSLMIB	draft-ietf-adslmib-vdsl-08	18/04	Definitions of Managed Objects for VDSL
ASCERTE	draft-dickel-ascertech-base-00	16/04	Ascertech's Billing and Accounting System Exchange Protocol
AVT	draft-ietf-avt-rtp-retransmission-07	04/04	RTP Retransmission Payload Format
	draft-ietf-avt-rtcp-report-extns-04	17/04	RTP Control Protocol Extended Reports (RTCP XR)
	draft-ietf-avt-rtp-clearmode-00	07/04	RTP payload format for a 64 kbit/s transparent call
BGP4	draft-ietf-idr-bgp4-20	31/03	A Border Gateway Protocol 4 (BGP-4)
	draft-ietf-idr-bgp-identifier-02	04/04	AS-wide Unique BGP Identifier for BGP-4
	draft-ietf-idr-bgp-analysis-02	23/04	BGP-4 Protocol Analysis
	draft-shankar-bgp-reference-capability-00	25/03	BGP-4 Reference Attribute Capability
	draft-mcpherson-bgp4-expereince-00	24/04	Experience with the BGP-4 Protocol
CDI	draft-ietf-cdi-known-request-routing-03	04/04	Known CN Request-Routing Mechanisms
CGI	draft-coar-cgi-v11-03	16/04	The Common Gateway Interface (CGI) Version 1.1
CHARTER	draft-iesg-charter-02	09/04	An IESG charter
CMS	draft-housley-cms-fw-wrap-01	01/04	Using CMS to Protect Firmware Packages
CWC	draft-irtf-cfrg-cwc-00	14/04	The CWC-AES Dual-Use Mode
DCLOR	draft-swami-tsvwg-tcp-dclor-01	01/04	De-correlated Loss Rec. using SACK option for spurious timeouts
DHCP	draft-ietf-dhc-dhcpv6-opt-cliprefprefix-01	21/03	Client Preferred Prefix option for DHCPv6
	draft-ietf-dhc-unused-optioncodes-02	16/04	Unused DHCP Option Codes
	draft-ietf-dhc-dhcpv6-interop-01	08/04	Results from Interoperability Tests of DHCPv6 Implementations
	draft-ietf-dhc-dhcpv6-stateless-00	07/04	A Guide to Implementing Stateless DHCPv6 Service
	draft-volz-dhc-dhcpv6-site-options-00	07/04	Site Specific Options for DHCP for IPv6
DIFF	draft-deoliveira-diff-te-preemption-01	21/03	LSP Preemption policies for Diff-Serv-aware MPLS Traffic Enginee.
DIFFSER	draft-silverman-diffserv-mlefphb-01	08/04	Multi-Level Expedited Forwarding
DNS	draft-ietf-dnsext-unknown-rrs-05	26/03	Handling of Unknown DNS Resource Record Types
	draft-ietf-dnsext-mdns-17	17/04	Linklocal Multicast Name Resolution (LLMNR)
	draft-ietf-dnsop-inaddr-required-04	28/03	Requiring DNS IN-ADDR Mapping
	draft-josefsson-dns-url-07	21/04	Domain Name System Uniform Resource Identifiers
DSP	draft-fecyk-dsprotocol-01	10/04	DSP A Way to Identify Hosts Authorized to Send SMTP Traffic
DSR	draft-ietf-manet-dsr-09	16/04	The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks
DTNRG	draft-irtf-dtnrg-bundle-spec-00	24/03	Bundle Protocol Specification
	draft-irtf-dtnrg-ipn-bundle-xfer-00	24/03	Delay-Tolerant Network Interplanetary Internet Bundle Transfer
	draft-irtf-dtnrg-arch-00	24/03	Delay-Tolerant Network Architecture
EAP	draft-vollbrecht-eap-state-02	24/04	State Machines for EAP Peer and Authenticator
	draft-tschofenig-eap-ikev2-00	24/04	EAP IKEv2 Method (EAP-IKEv2)
EDIINT	draft-ietf-ediint-compression-02	28/03	Compressed Data for EDIINT
EMAIL	draft-danisch-email-mtp-00	16/04	An advanced Mail Transfer Protocol
ENUM	draft-ietf-enum-rfc2916bis-05	08/04	The E.164 to URI DDDS Application (ENUM)
ENUMSER	draft-brandner-enumservice-vovi-01	21/03	Registration for enumservices voice and video
FAX	draft-ietf-fax-gateway-protocol-09	14/04	Internet FAX Gateway Functions
	draft-ietf-fax-gateway-options-06	14/04	Guideline of optional services for Internet FAX Gateway
	draft-ietf-fax-faxservice-enum-01	03/04	IFAX service of ENUM
FEC	draft-allan-fec-cv-overview-00	23/04	The FEC-CV proposed extension to the Y.1711 protocol
FHA	draft-park-fasthandover-agent-fmipv6-00	14/04	Fast Handover Agent (FHA) for Fast Router Discovery in FMIPv6
ICAP	draft-stecher-icap-subid-00	10/04	ICAP Extensions
IDN	draft-hoffman-idn-reg-00	25/03	Framework for Registering Internationalized Domain Names
	draft-josefsson-idn-test-vectors-00	27/03	Nameprep and IDNA Test Vectors
	draft-chung-idnop-charprep-00	01/04	CHARPREP – Character Equivalency Preparations for IDN
	draft-chung-idnop-zoneprep-00	01/04	ZONEPREP - Zone Preparations for IDN
	draft-chung-idnop-epp-idn-00	01/04	EPP Internationalized Domain Name Mapping
IEPREP	draft-ietf-ieprep-ets-telephony-03	18/04	IP Telephony Reqs for Emergency Telecommunication Service
IETF	draft-mrose-ietf-posting-00	16/04	A Practice for Revoking Posting Rights to IETF mailing lists
IMAA	draft-hoffman-imaa-01	18/04	Internationalizing Mail Addresses in Applications (IMAA)
IMAP	draft-ietf-imapext-condstore-01	21/04	IMAP Extension for Conditional STORE operation
	draft-leiba-imap-search-multiple-01	25/03	IMAP4 SEARCHM Command for Multiple Mailboxes
INTERNET	draft-iab-e2e-futures-02	22/04	The Rise of the Middle and the Future of End to End:
IP	draft-eastlake-ip-mime-07	21/04	IP over MIME
IPO	draft-ietf-ipo-framework-04	08/04	IP over Optical Networks: A Framework
	draft-ietf-ipoib-ip-over-infiniband-03	18/04	IP encapsulation and address resolution over InfiniBand networks
IPPM	draft-ietf-ippm-metrics-registry-04	18/04	IPPM metrics registry
IPR	draft-ietf-ipr-wg-guidelines-03	22/04	Guidelines for Working Groups on Intellectual Property Issues
	draft-ietf-ipr-technology-rights-05	22/04	Intellectual Property Rights in IETF Technology
	draft-ietf-ipr-submission-rights-04	21/04	IETF Rights in Submissions



	draft-savola-ipr-lastcall-00	24/04	Mentioning IPR Considerations in Last Calls
IPV6	draft-ietf-ipv6-flow-label-07	11/04	IPv6 Flow Label Specification
	draft-ietf-multi6-multihoming-reqs-05	17/04	Goals for IPv6 Site-Multihoming Architectures
	draft-hain-ipv6-pi-addr-04	17/04	An IPv6 Provider-Independent Global Unicast Address Format
	draft-hain-ipv6-pi-addr-use-04	17/04	Applic. & Use of the IPv6 Provider Ind. Global Unicast Add. Fmt
	draft-rjaya-ct-fmip6-l2st-ant-ho-00	31/03	Context Transfer & Fast Mobile IPv6 Interactions in a L2 Source-..
	draft-hain-ipv6-sitelocal-00	07/04	Site-Local Requirements
	draft-baker-ipv6-renumber-procedure-00	11/04	Procedures for Renumbering an IPv6 Network without a Flag Day
	draft-jeong-ipv6-ra-dns-autoconf-00	18/04	IPv6 Router Advertisement based DNS Autoconfiguration
	draft-park-ipv6-extensions-dns-pnp-00	21/04	IPv6 Extensions for DNS Plug and Play
ISIS	draft-ietf-isis-wg-mib-12	04/04	Management Information Base for IS-IS
	draft-ietf-isis-wg-multi-topology-06	26/03	M-ISIS: Multi Topology (MT)Routing in IS-IS
	draft-ietf-isis-igp-p2p-over-lan-02	26/03	Point-to-point operation over LAN in link-state routing protocols
	draft-ietf-isis-auto-encap-03	31/03	IS-IS Automatic Encapsulation
LDAP	draft-rharrison-ldap-intermediate-resp-01	28/03	The LDAP Intermediate Response Message
	draft-hall-ldap-audit-00	31/03	Generalized Audit object class & generalized AuditEvent attribute
LIBERTY	draft-mealling-liberty-urn-00	11/04	A URN Namespace For The Liberty Alliance Project
LMP	draft-ietf-ccamp-lmp-08	26/03	Link Management Protocol (LMP)
	draft-ietf-ccamp-lmp-mib-05	21/04	LMP Management Information Base
	draft-ietf-ccamp-lmp-wdm-02	26/03	LMP for DWDM Optical Line Systems
	draft-ietf-ccamp-lmp-test-sonet-sdh-02	26/03	SONET/SDH Encoding for LMP Test messages
	draft-rbradfor-ccamp-lmp-lol-01	11/04	LMP Extensions for Link discovery Using Loss of Light
LUMAS	draft-cordell-lumas-00	08/04	A Language for Universal Message Abstraction & Specification
MEGACO	draft-ietf-megaco-h248v2-04	03/04	The Megaco/H.248v2 Gateway Control Protocol, version 2
MGCP	draft-foster-mgcp-returncodes-02	11/04	Media Gateway Control Protocol (MGCP) Return Code Usage
MGCP	draft-foster-mgcp-redirect-02	24/04	MGCP Redirect and Reset Package
MIB	draft-ietf-disman-alarm-mib-11	17/04	Alarm MIB
	draft-ietf-disman-conditionmib-08	17/04	Alarm Reporting Control MIB
	draft-ietf-hubmib-wis-mib-07	21/03	Def. of Managed Objects for the Ethernet WAN Interface Sublayer
MIDCOM	draft-barnes-midcom-mib-00	31/03	Managed Objects for Middlebox Communications (MIDCOM)
MMS	draft-stebrose-lemonade-mmsarch-00	21/03	Mobile Messaging Architectures and Requirements
MMUSIC	draft-ietf-mmusic-sdp-srcfilter-04	16/04	Session Description Protocol (SDP) Source Filters
	draft-ietf-mmusic-offer-answer-examples-00	24/04	Session Description Protocol Offer Answer Examples
	draft-levin-mmusic-xml-media-control-02	07/04	XML Schema for Media Control
MPLS	draft-ietf-ccamp-gmpls-architecture-05	24/03	Generalized Multi-Protocol Label Switching Architecture
	draft-ietf-mpls-tc-mib-06	02/04	Definitions of Textual for MPLS Management
	draft-ietf-mpls-ldp-dod-restart-00	18/04	LDP DoD Graceful Restart
	draft-ietf-mpls-nodeid-subobject-00	18/04	Definition of an RRO node-id subobject
	draft-ietf-mpls-oam-requirements-00	18/04	OAM Requirements for MPLS Networks
	draft-ietf-mpls-soft-preemption-00	18/04	MPLS Traffic Engineering Soft preemption
	draft-ietf-mpls-telink-mib-00	21/04	Traffic Engineering Management Information Base
	draft-allan-mpls-loadbal-04	15/04	Guidelines for MPLS Load Balancing
	draft-oki-ccamp-gmpls-ip-interworking-00	03/04	GMPLS and IP/MPLS Interworking Architecture
	draft-allan-mpls-pid-00	03/04	MPLS and IP PW Payload ID
	draft-papadimitriou-ccamp-gmpls-ason-req-00	10/04	Requirements for GMPLS Usage and Extensions for ASON
	draft-allan-mpls-a-bit-00	23/04	The Case for the 'A' Bit in the MPLS and IP PID
MSDP	draft-ietf-msdp-spec-15	02/04	Multicast Source Discovery Protocol (MSDP)
MSGHEAD	draft-newman-msgheader-originfo-05	28/05	Originator-Info Message Header
MSNIP	draft-ietf-magma-msnip-03	03/04	Multicast Source Notification of Interest Protocol (MSNIP)
MSSF	draft-ietf-magma-msf-api-04	21/03	Socket Interface Extensions for Multicast Source Filters
MUPDATE	draft-siemborski-mupdate-03	24/04	The MUPDATE Distributed Mailbox Database Protocol
MXCAST	draft-boudani-mxcast-00	22/04	Using Recursive Xcast Packets for Multicast Delivery
NDMP	draft-skardal-ndmpv4-04	31/03	Network Data Management Protocol Version 4
NEMO	draft-thubert-nemo-ipv4-traversal-00	21/03	IPv4 traversal for MIPv6 based Mobile Routers
	draft-paakkonen-nemo-prefix-delegation-00	25/03	Mobile Network Prefix Delegation extension for Mobile IPv6
NETDIS	draft-bichot-network-discovery-protocol-01	21/03	Network Discovery Protocol (NETDIS)
NETWORK	draft-breit-network-perf-throughput-00	10/04	Network Throughput and Performance Calculations
	draft-holness-network-l2vpsp-00	21/04	The Nortel Networks Ethernet L2 Virtual Private Service Protocol
NEWS	draft-kohn-news-article-03	28/03	News Article Format
NNTP	draft-ietf-usefor-article-10	07/04	News Article Format
NSIS	draft-ietf-nsis-qos-requirements-00	04/04	Requirements of a QoS Solution for Mobile IP
NSRG	draft-irtf-nsrg-report-09	27/03	What's In A Name:Thoughts from the NSRG
ODMRP	draft-yi-manet-odmrp-00	31/03	On-Demand Multicast Routing Protocol for Ad Hoc Networks
OLSR	draft-ietf-manet-olsr-09	15/04	Optimized Link State Routing Protocol
OPES	draft-rousskov-opes-ocp-00	02/04	OPES Callout Protocol (OCP)
OSPF	draft-nguyen-ospf-lls-02	03/04	OSPF Link-local Signaling
	draft-nguyen-ospf-oob-resync-02	03/04	OSPF Out-of-band LSDB resynchronization
	draft-nguyen-ospf-restart-02	03/04	OSPF Restart Signaling
	draft-thorup-ospf-harmful-00	23/04	OSPF Areas Considered Harmful
	draft-ietf-ospf-ospfv3-mib-06	07/04	Management Information Base for OSPFv3
	draft-pillay-esnault-ospf-flooding-05	28/03	OSPF Refresh and Flooding Reduction in Stable Topologies
	draft-ietf-ospf-mib-update-06	16/04	OSPF Version 2 Management Information Base
	draft-ietf-ospf-hitless-restart-07	26/03	Graceful OSPF Restart
	draft-ietf-ospf-scalability-03	01/04	Treatment of Specific OSPF Packets & Congestion Avoidance
	draft-ietf-ospf-ospfv3-auth-01	18/04	Authentication/Confidentiality for OSPFv3
	draft-ietf-ospf-ospfv3-traffic-00	17/04	Traffic Engineering Extensions to OSPF version 3
PANA	draft-ietf-pana-usage-scenarios-05	09/04	Problem Space and Usage Scenarios for PANA



PE	draft-guichard-pe-ce-addr-02	10/04	Address Allocation for PE-CE links within an RFC2547bis Network
PPP	draft-josefsson-pppext-eap-tls-eap-06	25/03	Protected EAP Protocol (PEAP)
	draft-song-pppext-sip-support-02	22/04	SIP server IPCP configuration option for PPP
	draft-shakeel-pppext-mlppp-lo-00	03/04	Enhanced ML PPP suitable for multiple scalable bandwidth links
PROVREG	draft-ietf-provreg-epp-09	21/03	Extensible Provisioning Protocol
	draft-ietf-provreg-epp-contact-07	24/04	Extensible Provisioning Protocol Contact Mapping
	draft-ietf-provreg-epp-domain-07	24/04	Extensible Provisioning Protocol Domain Name Mapping
	draft-ietf-provreg-epp-host-07	24/04	Extensible Provisioning Protocol Host Mapping
	draft-ietf-provreg-epp-ext-01	08/04	Guidelines for Extending the Extensible Provisioning Protocol
PWE3	draft-nadeau-pwe3-vccv-00	03/04	Pseudo Wire (PW) Virtual Circuit Connection Verification (VCCV)
	draft-nadeau-pwe3-oam-msg-map-00	03/04	Pseudo Wire (PW) OAM Message Mapping
	draft-ietf-pwe3-requirements-05	27/03	Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
	draft-ietf-pwe3-control-protocol-02	28/03	Pseudowire Setup and Maintenance using LDP
RMONMIB	draft-ietf-rmonmib-tpm-mib-08	18/04	Transport Performance Metrics MIB
RMT	draft-chiu-rmt-bb-track-00	07/04	Reliable Multicast Transport Building Block: TRACK Mechanisms
RMT	draft-sjkoh-rmt-bb-tree-config-00	07/04	Reliable Multicast Transport Building Block: TRACKConfiguration
ROHC	draft-ietf-rohc-rtp-rfc3095-interoperability-02	16/04	Interoperability of RFC 3095
	draft-ietf-rohc-udp-lite-00	11/04	RObust Header Compression (ROHC):Profiles for UDP-Lite
RPSEC	draft-ietf-rpsec-routing-threats-00	02/04	Generic Threats to Routing Protocols
RSS2	draft-nottingham-rss2-00	17/04	RSS 2.0
RSVP	draft-westberg-proposal-for-rsvpv2-nslp-00	17/04	A Proposal for RSVPv2-NSLP
SEAMOBY	draft-trossen-seamoby-dycard-01	01/04	A Dynamic Protocol for Candidate Access-Router Discovery
	draft-calhoun-seamoby-lwapp-00	02/04	Light Weight Access Point Protocol (LWAPP)
	draft-ietf-seamoby-mobility-terminology-03	03/04	Mobility Related Terminology
SIEVE	draft-murchison-sieve-subaddress-06	31/03	Sieve -- Subaddress Extension
	draft-daboo-sieve-spamtest-03	10/04	SIEVE Spamtest and Virustest Extensions
	draft-homme-sieve-variables-01	17/04	Sieve -- Variables Extension
	draft-daboo-sieve-include-00	10/04	SIEVE Include Extension
	draft-degener-sieve-copy-00	21/04	Sieve -- 'copy' extension
	draft-degener-sieve-editheader-00	21/04	Sieve -- 'editheader' extension
	draft-degener-sieve-multiscript-00	21/04	Sieve -- Sequential Execution of Multiple Scripts
SIGTRAN	draft-bidas-sigtran-sgsg-03	24/04	M3UA SG-SG communication
	draft-ietf-sigtran-signalling-over-sctp-appli-08	26/03	Telephony Signalling Transport over SCTP applicability statement
	draft-ietf-sigtran-m2pa-08	23/04	SS7 MTP2-User Peer-to-Peer Adaptation Layer
SIMPLE	draft-lonnfors-simple-binpidf-00	08/04	External Object Extension to Presence Information Data Format
	draft-mierla-simple-xmpp-interworking-00	23/04	SIMPLE-XMPP Interworking
	draft-ietf-simple-data-req-02	16/04	Requirements for Manipulation of Data Elements in SIP
	draft-ietf-simple-event-list-01	31/03	A SIP Event Notification Extension for Collections
SIP	draft-kaul-sip-fsm-framework-00	21/03	Finite State Machine (FSM) Framework for SIP Extensions
	draft-ietf-sipping-pstn-call-flows-02	07/04	Session Initiation Protocol PSTN Call Flows
	draft-ietf-sipping-basic-call-flows-02	07/04	Session Initiation Protocol Basic Call Flow Examples
	draft-ietf-sipping-qsig2sip-01	10/04	Interworking between SIP and QSIG
	draft-ietf-sipping-cc-conferencing-00	15/04	SIP Call Control - Conferencing for User Agents
	draft-ietf-sipping-conferencing-requir-00	24/04	High Level Requirements for Tightly Coupled SIP Conferencing
SMQP	draft-tegen-smqp-10	14/04	SMQP: Simple Message Queue Protocol
SMTP	draft-ietf-msgtrk-smtpext-05	01/04	SMTP Service Extension for Message Tracking
	draft-ietf-msgtrk-trkstat-05	01/04	An Extensible Message Format for Message Tracking Responses
SOAP	draft-baker-soap-media-reg-02	14/04	The 'application/soap+xml' media type
SSH	draft-ietf-secsh-break-00	08/04	Session Channel Break Extension
TBRPF	draft-ietf-manet-tbrpf-08	22/04	Topology Dissemination Based on Reverse-Path Forwarding
TCP	draft-swami-tcp-lmdr-00	28/03	Lightweight Mobility Detection and Response Algorithm for TCP
TEWG	draft-ietf-tewg-diff-te-russian-02	24/03	Russian Dolls Bandwidth Model for Diff-Serv MPLS Traffic Enginee
TEWG	draft-ietf-tewg-diff-te-mar-00	16/04	Max Allocation with Reservation Bandwidth Model for MPLS
UNICODE	draft-rmcgowan-unicode-procs-02	31/03	Unicode Consortium Procedures, Policies, Stability, Public Access
URI	draft-wilde-text-fragment-02	07/04	URI Fragment Identifiers for the text/plain Media Type
VPN	draft-marques-ppvpn-ibgp-00	23/04	RFC2547bis networks using internal BGP as PE-CE protocol
	draft-ietf-ppvpn-requirements-06	16/04	Service requirements for Layer 3 Provider Provisioned VPN
	draft-ietf-ppvpn-framework-08	26/03	A Framework for Layer 3 Provider Provisioned VPN
WEBDAV	draft-reschke-webdav-property-datatypes-04	24/03	Datatypes for WebDAV properties
	draft-ietf-webdav-ordering-protocol-07	24/03	WebDAV Ordered Collections Protocol
WHOIS	draft-sanz-whois-srv-00	07/04	Using DNS SRV records to locate whois servers
XMPP	draft-ietf-xmpp-im-09	22/04	XMPP Instant Messaging
	draft-ietf-xmpp-core-10	22/04	XMPP Core
	draft-ietf-xmpp-resourceprep-02	22/04	A Stringprep Profile for Resource Identifiers in XMPP
	draft-ietf-xmpp-nodeprep-02	22/04	Nodeprep: A Stringprep Profile for Node Identifiers in XMPP
XXX	draft-eastlake-xxx-05	16/04	.sex Considered Dangerous



NOS COMMENTAIRES

LES RFC

RFC 3511

Benchmarking Methodology for Firewall Performance

Ce RFC résulte de l'adoption de la proposition du groupe de l'IETF 'Benchmark' référencée '**draft-ietf-bmwg-firewall**'. Il propose un mode opératoire pour mesurer sans équivoque les performances d'un pare-feu et utilise la terminologie décrite dans le **RFC 2647**, intitulé «**Benchmarking Terminology for Firewall Performance**».

Son objectif est de définir une méthode fiable applicable à tout dispositif pare-feu pour en déterminer les performances. Les points mesurés par la méthode proposée sont les suivants :

- Le débit IP maximal,
- Le nombre de connexions TCP simultanées à travers le dispositif,
- Le taux maximal d'établissement de nouvelles connexions TCP,
- Le taux maximal de rejet de nouvelles connexions TCP,
- La résistance aux dénis de service.
- Le taux de transfert en protocole HTTP,
- Le nombre maximal de transaction HTTP,
- La gestion du trafic illicite,
- La gestion de la fragmentation IP,
- Le temps de latence introduit par la traversée du pare-feu

Les configurations physiques envisagées contiennent un pare-feu à deux ou trois interfaces, correspondant à un réseau interne, un réseau externe et éventuellement à une zone démilitarisée. Les règles de filtrage et de translation appliquées lors des tests telles qu'elles sont décrites sont basiques. En effet, ces tests étant destinés à être utilisés pour le plus grand nombre possible de pare-feu, seules les fonctionnalités supportées par tous seront utilisées.

On notera la présence de tests destinés à mesurer le comportement du pare-feu en présence de trafic HTTP illicite ainsi que sa robustesse face à des attaques de type déni de service, ici une attaque de type 'SynFlood'. Très utilisé, ce type d'attaque est désormais relativement bien gérée par les différents pare-feu.

Ce RFC a le mérite de proposer des méthodes standardisées là où chacun utilise des paramètres et des configurations différents. Nous regrettons par contre la disparition de toute référence aux protocoles **SMTP** et **FTP** initialement traités au même niveau que le protocole HTTP.

ftp://ftp.isi.edu/in-notes/rfc3511.txt

RFC 3514

The Security Flag in the IPv4 Header

Publié le 1 avril 2003, ce RFC propose d'ajouter dans les options du protocole IP un drapeau de sécurité. Ce drapeau binaire baptisé '**Evil bit**' doit permettre un filtrage plus efficace du trafic valide en rejetant tout paquet dont le drapeau aura été positionné par l'émetteur. S'appuyant sur une coopération efficace entre attaquants et attaqués, cette proposition d'implémentation pourrait bien rapidement se terminer en queue de poisson !

ftp://ftp.isi.edu/in-notes/rfc3514.txt



ALERTES ET ATTAQUES

ALERTES

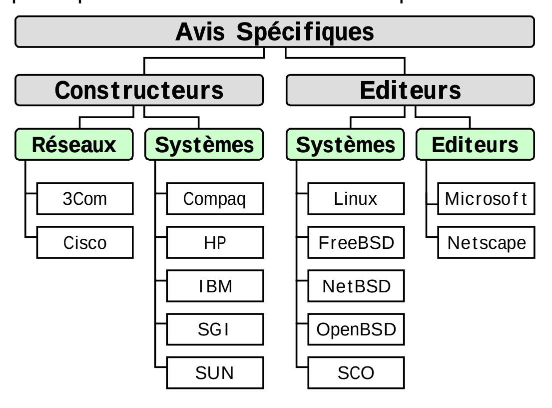
GUIDE DE LECTURE

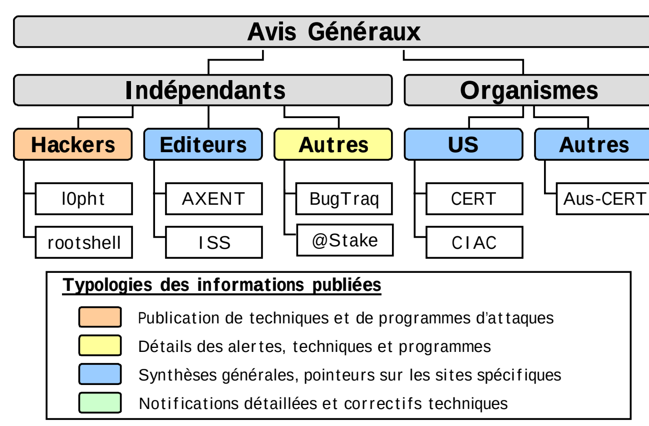
La lecture des avis publiés par les différents organismes de surveillance ou par les constructeurs n'est pas toujours aisée. En effet, les informations publiées peuvent être non seulement redondantes mais aussi transmises avec un retard conséquent par certains organismes. Dès lors, deux alternatives de mise en forme de ces informations peuvent être envisagées :

- Publier une synthèse des avis transmis durant la période de veille, en classant ceux-ci en fonction de l'origine de l'avis,
- Publier une synthèse des avis transmis en classant ceux-ci en fonction des cibles.

La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

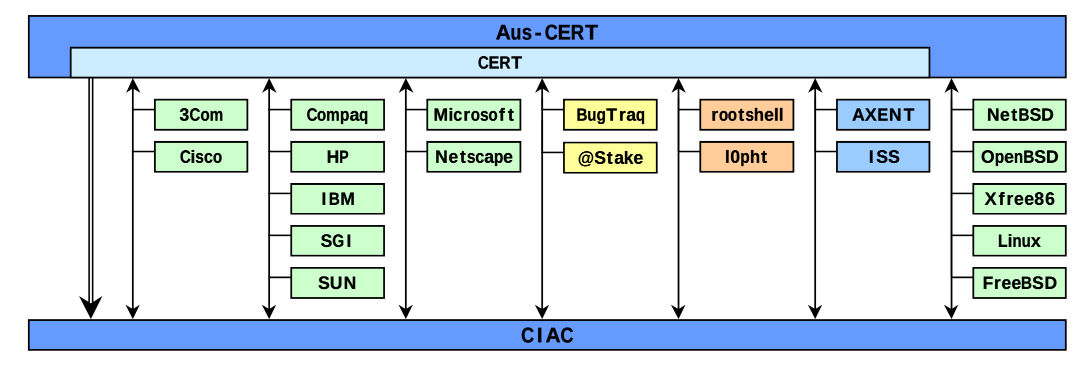
Afin de faciliter la lecture de ceux-ci, nous proposons un guide de lecture sous la forme d'un synoptique résumant les caractéristiques de chacune des sources d'information ainsi que les relations existant entre ces sources. Seules les organismes, constructeurs ou éditeurs, disposant d'un service de notification officiel et publiquement accessible sont représentés.





L'analyse des avis peut être ainsi menée selon les trois stratégies suivantes :

- Recherche d'informations générales et de tendances : Lecture des avis du CERT et du CIAC
- Maintenance des systèmes : Lecture des avis constructeurs associés
- Compréhension et anticipation des menaces : Lecture des avis des groupes indépendants





FORMAT DE LA PRESENTATION

Les alertes et informations sont présentées classées par sources puis par niveau de gravité sous la forme de tableaux récapitulatifs constitués comme suit :

❖ **Présentation des Alertes**

EDITEUR

TITRE		
Description sommaire		
Gravité · Date	Informations concernant la plate-forme impactée	
Correction	Produit visé par la vulnérabilité	Description rapide de la source du problème
Référence	URL pointant sur la source la plus pertinente	

❖ **Présentation des Informations**

SOURCE

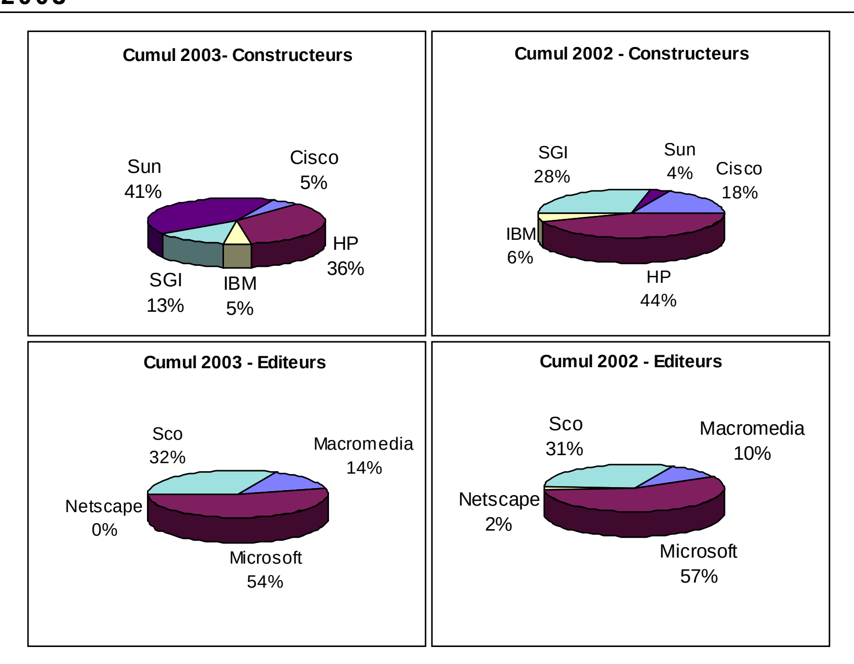
TITRE
Description sommaire
URL pointant sur la source d'information

SYNTHESE MENSUELLE

Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par les différents organismes. Ces chiffres ne sont donc représentatifs qu'en terme de tendance et d'évolution.

Période du **22/03/2003** au **25/04/2003**

		Cumul	
	Période	**2003**	**2002**
Organisme	**22**	**60**	**165**
CERT-CA	3	13	36
CERT-IN	0	0	7
CIAC	19	47	122
Constructeurs	**38**	**104**	**220**
Cisco	2	5	39
HP	9	37	99
IBM	1	5	13
SGI	8	14	61
Sun	18	43	8
Editeurs	**9**	**28**	**127**
Macromedia	1	4	13
Microsoft	6	15	72
Netscape	0	0	2
Sco	2	9	40
Unix libres	**69**	**190**	**349**
Linux RedHat	20	49	102
Linux Debian	30	83	120
Linux Mandr.	17	50	85
FreeBSD	2	8	42
Autres	**3**	**15**	**44**
@Stake	3	9	9
eEye	0	1	13
X-Force	0	5	22





ALERTES DETAILLEES

AVIS OFFICIELS

Les tables suivantes présentent une synthèse des principales alertes de sécurité émises par un organisme fiable, par l'éditeur du produit ou par le constructeur de l'équipement. Ces informations peuvent être considérées comme fiables et authentifiées. En conséquence, les correctifs proposés, s'il y en a, doivent immédiatement être appliqués.

AMAVIS

Relayage d'e-mails via Amavis-ng			
Un problème dans Amavis-ng autorise le relayage d'e-mail.			
Forte	10/04	Amavis Amavis-ng versions 0.1.6.1 à 0.1.6.3	
Correctif existant		'amavis-ng'	Mauvaise interaction entre Amavis-ng et Postfix
AMaViS		http://amavis.sourceforge.net/	
SF 7306		http://www.securityfocus.com/bid/7306	

APACHE

Multiples vulnérabilités dans Apache			
Plusieurs vulnérabilités du serveur Apache ont été révélées avec la publication de la version 2.0.45.			
Forte	03/04	Apache 2.0.44 et précédents, toutes plates-formes	
Correctif existant		Serveur Apache	Gestion des descripteurs de fichier
Apache		http://www.apache.org/dist/httpd/Announcement2.html	

APPLE

Augmentation de privilèges sur MacOS X			
Le service 'DirectoryService' de MacOS X permet à un utilisateur local d'acquérir les privilèges root.			
Forte	10/04	Apple MacOS X, 10.2.4 et précédents	
Correctif existant		'DirectoryService'	Exécution de fichier non contrôlé
@Stake		http://www.atstake.com/research/advisories/2003/a041003-1.txt	

Exposition d'informations des dossiers 'DropBox'			
Un utilisateur non privilégié peut modifier les permissions d'un dossier 'DropBox' afin d'en révéler son contenu.			
Moyenne	14/04	Apple MacOS X versions 10.0 à 10.2.4, MacOS X Server versions 10.0 à 10.2.4	
Correctif existant		Service de partage de fichiers	Modification des permissions d'un dossier 'DropBox'
Apple		http://www.info.apple.com/usen/security/security_updates.html	

Débordement de buffer dans QuickTime			
Le lecteur QuickTime contient un débordement de buffer.			
Moyenne	31/03	Apple QuickTime 5.x et 6.0 sur Windows	
Correctif existant		Traitement de l'URL	Débordement de buffer
iDefense		http://www.idefense.com/advisory/03.31.03.txt	

BEA

Vulnérabilité dans WebLogic			
Une vulnérabilité dans WebLogic permet à un utilisateur de contourner l'authentification pour accéder à certaines applications.			
Forte	26/03	BEA WebLogic 7.0 et 7.0.0.1 (toute plate-forme)	
Correctif existant		Cache de l'authentification	Non réinitialisation du cache
BEA03-27.00		http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/BEA03-27.jsp	

CISCO

Débordement de buffer dans CS ACS			
Le service d'administration Cisco Secure Access Control Server contient un débordement de buffer exploitable pour exécuter du code arbitraire.			
Critique	23/04	Cisco Secure ACS jusqu'aux versions 2.6.4, 3.0.3 et 3.1.1 comprises, sur plates-formes Windows	
Correctif existant		Service d'administration HTTP	Débordement de buffer
CSCea51366		http://www.cisco.com/warp/public/707/cisco-sa-20030423-ACS.shtml	
CIAC N-079		http://www.ciac.org/ciac/bulletins/n-079.shtml	



Contournement de l'authentification sur CatOS		
Une personne ayant accès en ligne de commande à un commutateur Catalyst peut accéder au mode privilégié sans connaître le mot de passe.		
Forte 24/04	Cisco Catalyst 4000, 6000 et 6500 utilisant CatOS 7.5(1)	
Correctif existant	Authentification de l'utilisateur	Non disponible
CSCea42030	http://www.cisco.com/warp/public/707/cisco-sa-20030424-catos.shtml	

DNS

Déni de service sur certains serveurs DNS		
Une réponse NXDOMAIN incorrecte lors d'une requête AAAA peut provoquer un déni de service.		
Moyenne 26/03	Serveurs DNS (non déterminé)	
Aucun correctif	Serveurs DNS	Message d'erreur inapproprié
CERT VU#714121	http://www.kb.cert.org/vuls/id/714121	

GAIM-ENCRYPT.

Débordement de buffer dans le module 'gaim-encryption'		
Un débordement de buffer affecte à distance le module 'gaim-encryption'.		
Moyenne 15/04	gaim-encryption 1.15 et inférieurs	
Correctif existant	Module Gaim-Encryption	Débordement de buffer
Rapid7 R7-0013	http://www.rapid7.com/advisories/R7-0013.html	

HP

Vulnérabilité du serveur 'CIFS/9000'		
Le serveur CIFS est vulnérable au même débordement de buffer que Samba.		
Critique 09/04	HP HP-UX 11.10, 11.11 et 11.22 utilisant un serveur CIFS/9000	
Correctif existant	Serveur 'CIFS/9000'	Débordement de buffer
HPSBUX0304-254	http://europe-support2.external.hp.com/	

Vulnérabilité du serveur FTP		
Le serveur FTP des systèmes MPE/iX contient une vulnérabilité permettant certains accès non autorisés.		
Forte 31/03	HP MPE/iX 5.5 6.X et 7.X sur HP3000.	
Correctif existant	Service FTP	Non disponible
HPSBMP0303-016	http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMP0303-016	

KDE

Exécution de commandes arbitraires dans KDE		
Une vulnérabilité dans KDE permet d'exécuter des commandes arbitraires lors du traitement des fichiers PostScript ou PDF.		
Forte 14/04	KDE 2 et 3 jusqu'à la version 3.1.1 incluse, Linux Debian 3.0 (woody)	
Correctif existant	KDE 'ghostscript'	Mauvais traitement des fichiers au format PS ou PDF
DSA-284-1	http://www.debian.org/security/2003/dsa-284	
KDE 20030409-1	http://www.kde.org/info/security/advisory-20030409-1.txt	

LINUX CALDERA

Vulnérabilité dans 'apcupsd'		
Le service 'apcupsd' contient plusieurs débordements de buffer.		
Critique 25/03	Caldera OpenLinux Server 3.1 et 3.1.1	
Correctif existant	Service 'apcupsd'	Débordements de buffer
CSSA-2003-015.0	ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2003-015.0.txt	

LINUX DEBIAN

Diverses vulnérabilités dans 'bonsai'		
L'outil d'interrogation de base CVS 'bonsai' contient plusieurs vulnérabilités.		
Critique 21/03	bonsai, sur Debian paquetages inférieurs au1.3+cvs20020224-1woody1 ou au 1.3+cvs20030317-1	
Correctif existant	'bonsai'	Non disponible
DSA-265-1	http://www.debian.org/security/2003/dsa-265	

Débordement de buffer dans 'epic'		
Le paquetage 'epic' est vulnérable à un débordement de buffer.		
Forte 15/04	Debian Linux 2.2 (potato) et 3.0 (woody)	
Correctif existant	Paquetage 'epic'	Débordement de buffer
DSA-287-1	http://www.debian.org/security/2003/dsa-287	



Vulnérabilité dans 'rinetd'		
Une vulnérabilité du serveur 'rinetd' peut conduire à un déni de service et à l'exécution de code arbitraire.		
Forte 17/04	Debian Linux 2.2 (potato) et 3.0 (woody)	
Correctif existant	Serveur 'rinetd'	Mauvais redimensionnement de la liste des connexions
DSA-289-1	http://www.debian.org/security/2003/dsa-289	

Modification des mots de passe dans 'ecartis'		
Une faille dans 'ecartis' permet de modifier les mots de passe utilisés.		
Moyenne 28/03	Debian Linux 2.2 (potato) et 3.0 (woody)Gestionnaires de listes de diffusion 'ecartis' et 'listar'	
Correctif existant	Paquetages 'ecartis' et 'listar'	Non disponible
DSA-271-1	http://www.debian.org/security/2003/dsa-271	

Vulnérabilité dans 'metrics'		
L'utilitaire 'metrics' contient une vulnérabilité permettant à un utilisateur local d'écraser des fichiers appartenant à la personne exécutant 'metrics'.		
Moyenne 07/04	'metrics', paquetages inférieurs à la version 1.0-1.1	
Correctif existant	Scripts 'halstead', 'gather_stats'	Conflit d'accès aux fichiers temporaires
DSA-279-1	http://www.debian.org/security/2003/dsa-279	

Création non sécurisée de fichiers dans 'gs-common'		
Le paquetage 'gs-common'peut être utilisé via 'ps2epsi' afin d'écraser un fichier arbitraire.		
Moyenne 14/04	Debian Linux 3.0 (woody)	
Correctif existant	Script 'ps2epsi'	Création non sécurisée de fichiers temporaires
DSA-286-1	http://www.debian.org/security/2003/dsa-286	

Création non sécurisée de fichiers dans LPRng		
Le paquetage LPRng peut être utilisé via 'psbanner' afin d'écraser un fichier arbitraire.		
Moyenne 15/04	Debian Linux 3.0 (woody)	
Correctif existant	'psbanner'	Création non sécurisée de fichiers temporaires
DSA-285-1	http://www.debian.org/security/2003/dsa-285	

Débordement de buffer dans 'ircii'		
Un débordement de buffer dans 'ircii' permet à un serveur de provoquer l'exécution de code arbitraire par un client se connectant.		
Moyenne 21/04	ircii, sur Debian, paquetages inférieurs aux 4.4M-1.1,20020322-1.1 ou 20030315-1	
Correctif existant	'ircii'	Débordement de buffer
DSA-291-1	http://www.debian.org/security/2003/dsa-291	

Vulnérabilité dans le paquetage 'mime-support'		
Le programme 'run-mailcap' du paquetage 'mime-support' créé des fichiers temporaires de manière non sécurisée.		
Moyenne 22/04	Paquetage mime-support, versions précédentes aux 3.18-1.1,3.9-1.1 et 3.22-1	
Correctif existant	Programme 'run-mailcap'	Création non sécurisée de fichiers temporaires
DSA-292-1	http://www.debian.org/security/2003/dsa-292	

Vulnérabilité dans 'gkrellm-newsticker'		
Deux vulnérabilités permettent de provoquer l'exécution de commandes ou de provoquer un déni de service.		
Moyenne 23/04	Systèmes 'gkrellm' utilisant gkrellm-newsticker	
Correctif existant	Module 'gkrellm-newsticker'	Mauvais filtrage de caractères vers l'interpréteur de commandes
DSA-294-1	http://www.debian.org/security/2003/dsa-294	

LINUX REDHAT

Vulnérabilité dans 'squirrelmail'		
Une nouvelle vulnérabilité de type 'Cross Site Scripting' été découvertes dans 'squirrelmail'.		
Forte 24/04	Squirrelmail 1.2.10 et précédents	
Correctif existant	'squirrelmail'	Mauvais échappement des données fournies par l'utilisateur
RHSA-03:112-03	https://rhn.redhat.com/errata/RHSA-2003-112.html	

Vulnérabilité dans EOG		
Le composant 'Eye Of Gnome' (EOG) contient une vulnérabilité permettant l'exécution de code non sollicité.		
Forte 03/04	EOG version 2.2.0 et précédents	
Correctif existant	Traitement des noms de fichiers	Non disponible
CIAC N-071	http://www.ciac.org/ciac/bulletins/n-071.shtml	
RHSA-03:128-07	https://rhn.redhat.com/errata/RHSA-2003-128.html	



Vulnérabilité de Mutt répercutée dans 'balsa'			
Le client de messagerie graphique 'balsa' réutilise du code provenant de Mutt et est ainsi vulnérable au même débordement de buffer. Une autre vulnérabilité a également été découverte.			
Moyenne	03/04	Balsa 1.2 et supérieurs, libesmtp 0.8.11 et inférieurs	
Correctif existant		1 - Connexions IMAP 2 - Bibliothèque 'libsmtp'	Débordements de buffer
RHSA-03:109-12		https://rhn.redhat.com/errata/RHSA-2003-109.html	

Vulnérabilités dans 'NetPBM'			
La bibliothèque 'NetPBM' contient des vulnérabilités pouvant être exploitées par un utilisateur local.			
Moyenne	03/04	NetPBM	
Correctif existant		Bibliothèque 'NetPBM'	Non disponible
RHSA-03:060-09		https://rhn.redhat.com/errata/RHSA-2003-060.html	

Déni de service via GtkHTML			
Une faille dans GtkHTML peut conduire à un déni de service du composant Evolution.			
Moyenne	15/04	Red Hat Linux 9	
Correctif existant		Outil 'GtkHTML'	Mauvaise gestion des messages au format HTML
RHSA-03:126-06		https://rhn.redhat.com/errata/RHSA-2003-126.html	

Vulnérabilités dans 'mgetty'			
Plusieurs vulnérabilités existent dans 'mgetty'.			
Faible	08/04	mgetty, versions 1.1.29 et précédents	
Correctif existant		mgetty	Débordement de buffer, Permissions laxistes
RHSA-03:036-10		https://rhn.redhat.com/errata/RHSA-2003-036.html	

MACROMEDIA

Exposition d'informations via les bannières Flash			
Certaines bannières Flash ne validant pas les URLs utilisées par le paramètre 'clickTAG' peuvent exposer certaines informations peu sensibles.			
Faible	11/04	Macromedia Flash (fichiers SWF)	
Correctif existant		'clickTAG' d'un élément Flash	Mauvaise implémentation des bannières de publicité au format Flash
Macromedia		http://www.macromedia.com/support/flash/ts/documents/clicktag_security.htm	

MICROSOFT

Vulnérabilité dans la machine virtuelle Java			
Une vulnérabilité dans la Machine Virtuelle Java de Microsoft permet à une applet de contourner les mécanismes de protection.			
Critique	09/04	Microsoft, tout système utilisant une version de la Machine Virtuelle Java (JVM) inférieure à la 3810	
Correctif existant		Vérificateur de code	Erreur d'implémentation
MS03-011		http://www.microsoft.com/technet/security/bulletin/MS03-011.asp	
CIAC N-074		http://www.ciac.org/ciac/bulletins/n-074.shtml	

Débordement de buffer dans le noyau Windows			
Un débordement de buffer affecte le noyau des systèmes Windows.			
Forte	16/04	Microsoft Windows NT 4.0, NT 4.0 Server, 2000 et XP	
Correctif existant		Noyau Windows (ntoskrnl.exe)	Débordement de buffer
CERT VU#446338		http://www.kb.cert.org/vuls/id/446338	
Entercept 04-16		http://www.entercept.com/news/uspr/04-16-03.asp	
MS03-013		http://www.microsoft.com/technet/security/bulletin/MS03-013.asp	

Multiples vulnérabilités dans Internet Explorer			
Plusieurs vulnérabilités dans Internet Explorer ont été publiées, dont la plus sévère permet l'exécution de code arbitraire sur le système de l'utilisateur.			
Forte	23/04	Microsoft Internet Explorer 5.01 SP3, 5.5 SP2 et 6.0 SP1	
Correctif existant		1 - Bibliothèque 'URLMON.DLL' 2 - Contrôle 'File Upload' 3 – Modules de visualisation 4 - Boîtes de dialogues	1 - Débordement de buffer 2 - Mauvais cloisonnement du contrôle 3 - Mauvais filtrage des paramètres 4 - Mauvais filtrage des paramètres
MS03-015		http://www.microsoft.com/technet/security/bulletin/MS03-015.asp	

Déni de service contre MS Proxy et ISA Server			
Les deux logiciels MS Proxy et ISA Server contiennent une vulnérabilité permettant à un attaquant situé sur le réseau interne de provoquer un déni de service.			
Moyenne	09/04	Microsoft Proxy Server 2.0Microsoft ISA Server	
Correctif existant		Service 'winsock'	Consommation excessive de ressources
MS03-012		http://www.microsoft.com/technet/security/bulletin/MS03-012.asp	



Vulnérabilité dans Outlook Express			
Il est possible de provoquer l'exécution de script dans la zone de sécurité locale.			
Moyenne	23/04	Microsoft Outlook Express 5.5 et 6.0	
Correctif existant		Gestion des URL 'MHTML'	Ouverture de fichiers locaux
MS03-014		http://www.microsoft.com/technet/security/bulletin/MS03-014.asp	

MUTT

Débordement de buffer dans Mutt			
Un débordement de buffer existe dans Mutt et est exploitable par un serveur IMAP.			
Faible	24/03	Mutt 1.4 et précédents	
Correctif existant		Connexions IMAP	Débordement de buffer
SuSE-SA:03:020		http://www.suse.de/de/security/2003_020_mutt.html	

ORACLE

Vulnérabilité dans 'Report Review Agent'			
Une vulnérabilité dans le composant 'Report Review Agent' permet à un utilisateur d'accéder à des fichiers restreints.			
Forte	10/04	Oracle E-Business Suite 11i, R1 à R8, Oracle Applications 10.7 et 11.0	
Correctif existant		'Report Review Agent'	Usurpation de requêtes
Oracle [#53]		http://otn.oracle.com/deploy/security/pdf/2003alert53.pdf	

OpenSSH/PAM

Prédiction d'informations sur les utilisateurs			
Une analyse des temps de réponse lors de la phase d'authentification via PAM ou OpenSSH permet de prédire certaines informations.			
Moyenne	15/04	OpenSSH version 2.2 à 3.0.2PAM (Pluggable Authentication Modules)	
Aucun correctif		Phase d'authentification	Attaques basées sur le temps de réponse
S.Krahmer		http://stealth.7350.org/epta.tgz	
SF 7342 et 7343		http://www.securityfocus.com/bid/7342	

REAL NETWORKS

Vulnérabilité dans RealPlayer et RealOne			
Il est possible de provoquer l'exécution de code arbitraire à la lecture d'un fichier '.png' piégé.			
Forte	27/03	RealPlayer 8 (version 6.0.9.584) et MacOS 9 RealOne player v1 sur Win32 (version 6.0.10.505) RealOne player v2 sur Win32 (versions 6.0.11.818, .830, .841 et .853) RealOne player sur MacOS X (versions 9.0.0.297 et 9.0.0.288) RealOne Enterprise Desktop sur Win32 (version 6.0.11.774) Cette liste n'est pas limitative, en particulier les versions antérieurs de RealPlayer semblent vulnérables bien que cela ne soit pas explicitement confirmé.	
Correctif existant		Décompression au format '.png'	Débordement de buffer
Real Networks		http://service.real.com/help/faq/security/securityupdate_march2003.html	

SAMBA

Débordement de buffer dans Samba			
Un nouveau débordement de buffer a été découvert dans Samba.			
Critique	07/04	Samba 2.2.8 et précédents	
Correctif existant		Samba	Débordement de buffer
DSA-280-1		http://www.debian.org/security/2003/dsa-280	
RHSA-03:137-09		https://rhn.redhat.com/errata/RHSA-2003-137.html	
SuSE-SA:03:025		http://www.suse.de/de/security/2003_025_smaba.html	
FreeBSD-SN03:01		http://www.linuxsecurity.com/advisories/freebsd_advisory-3128.html	
CIAC N-073		http://www.ciac.org/ciac/bulletins/n-073.shtml	

SENDMAIL

Débordement de buffer dans le traitement d'adresses e-mail			
Un débordement de buffer lors du traitement des adresses e-mail peut causer un déni de service ou l'exécution de code non sollicité avec les privilèges de l'utilisateur sous lequel tourne le service 'sendmail'.			
Critique	29/03	Sendmail jusqu'à la version 8.12.8 incluse, Sendmail Switch 2.1 avant la version 2.1.6 Sendmail Switch 3.0 avant la version 3.0.4 Sendmail pour NT 2.X avant la version 2.6.3	Sendmail Pro (toutes versions) Sendmail Switch 2.2 avant la version 2.2.6 Sendmail pour NT 3.0 avant la version 3.0.4
Correctif existant		Service 'sendmail'	Débordement de buffer
Sendmail		http://www.sendmail.org/8.12.9.html	
CERT VU#897604		http://www.kb.cert.org/vuls/id/897604	
CERT CA-2003-12		http://www.cert.org/advisories/CA-2003-12.html	



SETI@home

Vulnérabilité dans l'économiseur d'écran du SETI			
Le logiciel de calcul fourni comme économiseur d'écran par le SETI contient un débordement de buffer			
Forte	06/04	SETI@home 3.07 et précédents, toutes plateformes	
Correctif existant		Protocole de communication	Débordement de buffer
SETI		http://setiathome.ssl.berkeley.edu/version308.html	
Full Disclosure		http://lists.netsys.com/pipermail/full-disclosure/2003-April/009061.html	

SGI

Multiples vulnérabilités dans le serveur FTP			
Le serveur FTP de SGI contient plusieurs vulnérabilités.			
Forte	24/03	SGI IRIX 6.5.19f et précédents	
Correctif existant		1 & 2 - Serveur FTP3 - Client	1 - Conflit d'accès en mode FTP passif 2 - Absence de contrôle des arguments de la commande'PORT' 3 - Absence d'échappement des noms de fichiers téléchargés
SGI 030304-01-P		ftp://patches.sgi.com/support/free/security/advisories/20030304-01-P	

Vulnérabilités dans les fonctions RPC de la 'libc'			
La fonctions RPC de la bibliothèque 'libc' incluse dans IRIX contiennent deux vulnérabilités.			
Forte	08/04	SGI IRIX 6.5.19f et précédents	
Correctif existant		Bibliothèque 'libc'	Débordement de buffer
SGI 030402-01-P		ftp://patches.sgi.com/support/free/security/advisories/20030402-01-P	

Multiples vulnérabilités dans système d'impression LPR			
De multiples vulnérabilités affectent le sous système d'impression LPR.			
Forte	14/04	SGI IRIX versions 6.5 à 6.5.19	
Correctif existant		Sous système d'impression LPR	Multiples vulnérabilités
SGI 030406-01-P		ftp://patches.sgi.com/support/free/security/advisories/20030406-01-P	

SUN

Débordement de buffer dans le service LDAP			
Le service d'annuaire LDAP est vulnérable à un débordement de buffer exploitable localement.			
Forte	28/03	Sun Solaris 8 et 9 (Sparc et Intel)	
Palliatif proposé		Bibliothèque 'nss_ldap.so.1'	Débordement de buffer
Sun Alert 52222		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/52222	

Vulnérabilité dans 'newtask'			
La commande 'newtask' permet à un utilisateur local d'acquérir les privilèges root.			
Forte	28/03	Sun Solaris 9	
Correctif existant		Commande 'newtask'	Non disponible
Sun Alert 52111		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/52111	

Vulnérabilité dans 'dtsession'			
Un utilisateur local peut utiliser 'dtsession' pour acquérir les droits root.			
Forte	04/04	Sun Solaris 2.6 à 9 (Sparc et Intel)	
Correctif existant		Service 'dtsession'	Débordement de buffer
NsFocus		http://www.nsfocus.com/english/homepage/sa2003-03.htm	
CIAC N-072		http://www.ciac.org/ciac/bulletins/n-072.shtml	
Sun Alert 52388		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/52388	

Vulnérabilité dans 'lpq'			
Un débordement de buffer existe dans la commande 'lpq'			
Forte	31/03	Sun Solaris 2.6 et 7 (Sparc et Intel)	
Correctif existant		Commande 'lpq'	Débordement de buffer
Sun Alert 52443		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/52443	
CIAC N-068		http://www.ciac.org/ciac/bulletins/n-068.shtml	

Inefficacité de l'audit des sessions FTP anonymes			
Le mécanisme d'audit du module 'BSM' (Basic Security Module) ne fonctionne pas dans le cas des sessions FTP anonymes.			
Moyenne	18/04	Sun Solaris 2.5.1 à 8	
Correctif existant		Module 'BSM'	Défaut d'initialisation
Sun Alert 40521		http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/40521	



VIGNETTE

Vulnérabilité dans Vignette Story Server			
Une vulnérabilité dans Vignette Story Server permet d'obtenir des informations sensibles telles que des données sur d'autres sessions utilisateurs.			
Forte	07/04	Vignette Story Server versions 4.1 et 6	
Correctif existant		Interpréteur TCL	Débordement de buffer
@Stake		http://www.atstake.com/research/advisories/2003/a040703-1.txt	

XFS

Vulnérabilité dans le système de fichiers 'XFS'			
Le programme 'xfsdump' permet à un utilisateur local d'acquérir les privilèges root.			
Forte	11/04	SGI IRIX 6.5.19f et précédents, Linux Debian	
Correctif existant		Programme 'xfsdump'	Création de fichier non sécurisée
SGI 030404-01-P		ftp://patches.sgi.com/support/free/security/advisories/20030404-01-P	
DSA-283-1		http://www.debian.org/security/2003/dsa-283	

YABB

Vulnérabilité dans 'YABB SE'			
Le logiciel de gestion de forums 'YABB SE' contient une vulnérabilité permettant à un utilisateur de provoquer l'exécution de code PHP de son choix sur le serveur.			
Forte	22/04	YABB SE 1.5.1 et précédents	
Correctif existant		Fonction de personnalisation	Inclusion de données externes
NGSEC-2003-5		http://www.ngsec.com/docs/advisories/NGSEC-2003-5.txt	

ALERTES NON CONFIRMEES

Les alertes présentées dans les tables de synthèse suivantes ont été publiées dans diverses listes d'information mais n'ont pas encore fait l'objet d'une annonce ou d'un correctif de la part de l'éditeur. Ces alertes nécessitent la mise en place d'un processus de suivi et d'observation.

3COM

Vulnérabilités dans le serveur d'accès RAS 1500			
Le serveur d'accès RAS 1500 est sujet à un déni de service, et rend accessible sa configuration.			
Forte	24/03	3Com RAS 1500, firmware X2.0.10	
Correctif existant		1 - Pile IP 2 - Serveur HTTP embarqué	1 - Erreur de traitement 2 - Non protection de certaines pages
Bugtraq		http://www.securityfocus.com/archive/1/316043	
Bugtraq		http://www.securityfocus.com/archive/1/317769	

APACHE

Débordement de buffer dans le module 'mod_ntlm'			
Un débordement de buffer dans le module 'mod_ntlm' permet à un attaquant distant de provoquer l'exécution de code arbitraire.			
Critique	21/04	Module Apache mod_ntlm 0.4 et précédents et mod_ntlmv2 0.1	
Aucun correctif		Mécanisme de journalisation	Débordement de buffer
Bugtraq		http://www.securityfocus.com/archive/1/319239	

Déni de service via 'mod_access_referer'			
Le module Apache 'mod_access_referer' contient une vulnérabilité de déréférencement de pointeur NULL.			
Moyenne	17/04	Module 'mod_access_referer' 1.0.2	
Correctif existant		Module 'mod_access_referer'	Déréférencement de pointeur NULL
SafeMode		http://safemode.org/files/zillion/advisories/safemode-adv-marf.txt	

HP

Déni de service contre HP Instant TopTools			
Le programme de supervision HP Instant TopTools permet de provoquer le blocage du système sur lequel il est installé.			
Moyenne	31/03	HP Instant TopTools inférieur à la version 5.55	
Correctif existant		HP Instant TopTools	Consommation excessive de ressources par boucle infinie
Bugtraq		http://www.securityfocus.com/archive/1/316954	



IBM

Accès non autorisé via le service 'ftpd'		
Une vulnérabilité dans service 'ftpd' permet d'obtenir un accès non autorisé.		
Forte 14/04	IBM AIX 5.2	
Correctif existant	Service 'ftpd'	Mauvaise implémentation du processus d'authentification
SF 7346	http://www.securityfocus.com/bid/7346	

LINKSYS

Exposition du mot de passe des points d'accès LinkSys		
Les points d'accès sans fil LinkSys laissent transiter en clair le mot de passe administrateur.		
Forte 15/04	LinkSys (WAP11) version 2.2 Firmware 1.1	
Correctif existant	Points d'accès sans fil LinkSys	Non chiffrement du mot de passe
Securiteam	http://www.securiteam.com/securitynews/5ZP0D0U9PQ.html	

Non vérification de la clé publique du serveur RDP		
Les clients RDP ne vérifient pas la clé publique du serveur auquel ils se connectent.		
Forte 10/04	Microsoft Windows NT, 2000 et XP	
Aucun correctif	Clients RDP	Non vérification de la clé publique du serveur RDP
SF 7258	http://www.securityfocus.com/bid/7258	
Bugtraq	http://www.securityfocus.com/archive/1/317244	

Déni de service dans Internet Explorer		
Internet Explorer est vulnérable à un déni de service via la balise 'OBJECT'.		
Moyenne 16/04	Microsoft Internet Explorer 6.0 SP1 et inférieurs	
Aucun correctif	Navigateur Internet Explorer	Mauvaise gestion de la balise 'OBJECT'
Bugtraq	http://www.securityfocus.com/archive/1/318878	

NETGEAR

Non vérification du champ 'Host' sur les routeurs RP114		
Le serveurs web embarqué sur les routeurs NetGear RP114 ne vérifient pas le champ 'Host'.		
Moyenne 16/04	NetGear RP114 Cable/DSL Web Safe Router firmware 3.26	
Aucun correctif	NetGear RP114	Non vérification du champ 'Host'
Elaboration	http://elaboration.8bit.co.uk/projects/texts/advisories/netgear.logging.vulnerability.160403.txt	

PROGRESS

Débordement de buffer dans la base de données Progress		
Il existe un débordement de buffer dans la base de données Progress.		
Forte 09/04	Progress Database 8.3D, 8.3E, 8.3V et 9.1B, 9.1C, 9.1D	
Correctif existant	Variable d'environnement 'DLC'	Débordement de buffer
Bugtraq	http://www.securityfocus.com/archive/1/318300	
SF 7312	http://www.securityfocus.com/bid/7312	

SNORT

Débordement de buffer dans 'snort'		
Un débordement de buffer affecte le module Snort permettant de ré assembler le trafic TCP.		
Critique 15/04	Snort 2.0 versions inférieures à RC1Snort 1.8.x et 1.9.x	
Palliatif proposé	Module 'stream4 preprocessor'	Débordement de buffer
CORE-2003-0307	http://www.coresecurity.com/common/showdoc.php?idx=313&idxseccion=10	

STUNNEL

Vulnérabilité à l'attaque contre OpenSSL		
Stunnel utilise les bibliothèques d'OpenSSL et est donc vulnérable à la même attaque cryptographique.		
Forte 21/03	Stunnel jusqu'aux versions 3.22 et 4.04 comprises	
Correctif existant	Bibliothèque OpenSSL	Attaque par mesure du temps de réponse
Bugtraq	http://www.securityfocus.com/archive/1/315904	

AUTRES INFORMATIONS

REPRISES D'AVIS ET CORRECTIFS

Les vulnérabilités suivantes, déjà publiées, ont été mises à jour, reprises par un autre organisme, ou ont donné lieu à la fourniture d'un correctif :



APACHE

Détails concernant le déni de service

Comme annoncé lors la publication de Apache 2.0.45, des détails ont été publiés concernant le déni de service affectant les versions précédentes d'Apache 2, du à un excès d'allocation de mémoire. Notons qu'au moins un code d'exploitation a déjà été publié.

http://www.idefense.com/advisory/04.08.03.txt

CERT

Reprise de l'avis sur deux vulnérabilités de Snort

Le CERT a repris, sous la référence CA-2003-13, deux avis traitant d'un débordement de buffer dans deux pré processeurs du système de détection d'intrusion Snort. Les préprocesseurs 'stream4' et 'RPC' sont touchés par cette vulnérabilité exploitable à distance afin d'exécuter du code sous les droits 'root]

http://www.cert.org/advisories/CA-2003-13.html

CIAC

Reprise de l'avis MIT MITKRB5-SA-2003-005

Le CIAC a repris sous la référence N-062 l'avis MIT concernant un débordement de buffer dans Kerberos 5.

http://www.ciac.org/ciac/bulletins/n-062.shtml

Reprise de l'avis Microsoft MS03-008

Le CIAC a repris sous la référence N-063 l'avis de Microsoft concernant une vulnérabilité dans le moteur de scripts

http://www.ciac.org/ciac/bulletins/n-063.shtml

Reprise de l'avis SGI 20030404-01-P

Le CIAC a repris, sous la référence N-075, l'avis SGI 20030404-01-P traitant d'un problème dans le programme 'xfsdump'. Un utilisateur local peut exploiter cette vulnérabilité afin d'acquérir les privilèges 'root'.

http://www.ciac.org/ciac/bulletins/n-075.shtml

Reprise de l'avis SGI 20030406-01-P

Le CIAC a repris, sous la référence N-076, l'avis SGI 20030406-01-P au sujet de multiples vulnérabilités affectant le sous système d'impression LPR (bsdlpr) sur IRIX.

http://www.ciac.org/ciac/bulletins/n-076.shtml

Reprise de l'avis Microsoft MS03-013

Le CIAC a repris, sous la référence N-077, l'avis Microsoft MS03-013 au sujet d'un débordement de buffer dans le noyau des systèmes Windows (ntoskrnl.exe).

http://www.ciac.org/ciac/bulletins/n-077.shtml

Reprise de l'avis Snort 2003-04-16-1

Le CIAC a repris, sous la référence N-078, l'avis Snort [2003-04-16-1] au sujet du débordement de buffer dans le préprocesseur 'stream4'.

http://www.ciac.org/ciac/bulletins/n-078.shtml

Reprise de l'avis CERT CA-2003-11

Le CIAC a repris, sous la référence N-065, l'avis CERT [CA-2003-11] au sujet de nombreuses vulnérabilités affectant Lotus Notes et Domino.

http://www.ciac.org/ciac/bulletins/n-065.shtml

Reprise de l'avis de Real Networks sur RealPlayer

Le CIAC a repris sous la référence N-066 l'avis de Real Networks concernant une vulnérabilité dans RealPlayer et RealOne.

http://www.ciac.org/ciac/bulletins/n-066.shtml

Reprise de l'avis CERT CA-2003-12

Le CIAC a repris sous la référence N-067 l'avis du CERT concernant le débordement de buffer dans Sendmail.

http://www.ciac.org/ciac/bulletins/n-067.shtml

Reprise de l'avis Sun Alert ID 52111

Le CIAC a repris sous la référence N-069 l'avis de Sun concernant une vulnérabilité dans la commande 'newtask'.

http://www.ciac.org/ciac/bulletins/n-069.shtml

Reprise de l'avis Sun Alert ID 50161

Le CIAC a repris sous la référence N-070 l'avis de Sun concernant une vulnérabilité de la commande 'at'.

http://www.ciac.org/ciac/bulletins/n-070.shtml

Reprise de l'avis Microsoft MS03-014

Le CIAC a repris sous la référence N-081 l'avis de Microsoft à propos de plusieurs vulnérabilités dans Outlook Express.

http://www.ciac.org/ciac/bulletins/n-081.shtml

Reprise de l'avis Microsoft MS03-015

Le CIAC a repris sous la référence N-082 l'avis de Microsoft à propos de plusieurs vulnérabilités dans Internet Explorer. Microsoft [MS03-015]

http://www.ciac.org/ciac/bulletins/n-082.shtml



CLEARSWIFT

Correctif pour MAILSweeper

Clearswift a publié un correctif pour MAILSweeper, incapable de traiter des en-têtes MIME malformées. Le correctif met à jour les version 4.3.6 (SP1) en 4.3.7.

http://www.mimesweeper.com/download/bin/Patches/MAILsweeper_Patches_301_ReadMe.htm

FREEBSD

Disponibilité de plusieurs correctifs

FreeBSD annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

samba	*FreeBSD-SN-03:01*
seti@home	*FreeBSD-SN-03:02*
OpenSSL	*FreeBSD-SA-03:06*
sendmail	*FreeBSD-SA-03:07*

http://www.linuxsecurity.com/advisories/

HP

Correctifs pour Sendmail sur MPE/iX

HP a publié des correctifs pour Sendmail sur ses systèmes MPE/iX. Sendmail est vulnérable à un débordement de buffer dans le traitement des en-têtes.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMP0304-018

Révision du bulletin HPSBUX0208-209

HP a révisé le bulletin HPSBUX0208-209 au sujet des vulnérabilités affectant les résolveurs DNS et BIND. Cette révision indique que de nouveaux correctifs 'PHNE_27795' pour HP-UX 11.00 et 'PHNE_28450' pour HP-UX 11.11 ont remplacé les anciens.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0208-209

Révision du bulletin HPSBUX0304-253

HP a révisé le bulletin HPSBUX0304-253 au sujet d'une vulnérabilité dans 'sendmail'. Cette mise à jour indique une erreur de typographie sur le nom de fichier '/usr/newconfig/etc/mail/sendmail.cf'. Par ailleurs, les correctifs pour HP-UX 10.10 sont disponibles via la version Sendmail 8.8.6, directement accessible à l'adresse http://www.software.hp.com/products/Sendmail/index.html

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0304-253

Révision des bulletins HPSBUX0208-212 et HPSBUX0209-218

HP a révisé les bulletins HPSBUX0208-212 et HPSBUX0209-218 au sujet d'une vulnérabilité des imprimantes Jetdirect et Laserjet dans OpenSSL et dans le résolveur DNS. Ces mises à jour indiquent que les firmwares X.24.06 sont disponibles.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0208-212
http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0209-218

Correctifs pour 'CIFS/9000'

HP a révisé son bulletin [HPSBUX0304-254] pour indiquer la disponibilité de nouveaux correctifs.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0304-254

Correctifs pour diverses vulnérabilités sur Tru64

HP a publié de nouveaux correctifs pour la 'libc' de ses systèmes Tru64. Les vulnérabilités corrigées sont les suivantes : - débordement de buffer dans le résolveur DNS - vulnérabilité de la fonction 'calloc()' - débordement de buffer dans la fonction 'xdrmem_getbytes()' - dénis de service contre le service RPC Cette dernière vulnérabilité semble similaire à celle déjà connue sur Solaris. De plus, il est possible qu'elle soit également présente dans les systèmes HP-UX, bien que cela ne soit pas confirmé.

http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2003.0462.1

Correctif pour Sendmail

Hp a publié pour ses systèmes MPE/iX 7.0 et 7.5 un correctif pour Sendmail, sujet à un débordement de buffer dans le traitement des en-têtes.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMP0303-017

Mise à jour de l'avis sur 'xdrmem_getbytes()'

HP a mis à jour son avis sur la vulnérabilité affectant la fonction 'xdrmem_getbytes()'. La modification concerne le script d'installation des correctifs temporaires, pour lequel des commandes avaient été omises

http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0303-252

Correctif pour Sendmail

HP a publié des correctifs pour Sendmail pour ses systèmes HP-UX.

http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0304-253

Correctifs pour OpenSSL

HP a publié pour ses systèmes HP-UX 11.00, 11.11 et 11.22 des correctifs pour plusieurs vulnérabilités affectant OpenSSL. La première autorise des attaques cryptographiques basées sur le temps et la seconde permet d'attaquer les sessions SSL/TLS basées sur l'algorithme de chiffrement RSA et utilisant le padding décrit par PKCS#1.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0304-255



Correctif pour Apache

HP a publié un correctif pour Apache, correspondant à la version 2.0.45. Les versions 2.0.44 et précédentes sont sujettes à plusieurs vulnérabilités.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0304-256

IBM

Résumé des vulnérabilités de Lotus Notes et Domino

Le CERT/CC a publié un avis résumant les vulnérabilités de Lotus Notes et Domino récemment publiées et faisant le point sur les versions effectivement vulnérables. Sont reprises : - Les alertes initialement annoncées par NGSSoftware, auxquelles sont vulnérables les versions inférieures aux 5.0.12 et 6.0.1 de Lotus Notes. Une en particulier nécessite l'application du correctif CF1 après passage en version 6.0.1. - Les alertes initialement annoncées par Rapid7, auxquelles sont vulnérables les versions inférieures à la 5.0.12.

http://www.cert.org/advisories/CA-2003-11.html

Correctifs pour Sendmail

IBM a publié des correctifs pour Sendmail, sujet à un débordement de buffer dans le traitement des en-têtes. Ces correctifs sont disponibles pour AIX 4.3.3, 5.1.0 et 5.2.0.

http://www-1.ibm.com/services/continuity/recover1.nsf/MSS/MSS-OAR-E01-2003.0461.1

LINUX CALDERA

Disponibilité de nombreux correctifs

Caldera annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

OpenSSL	*CSSA-2003-013.0*
OpenSSL	*CSSA-2003-014.0*
apcupsd	*CSSA-2003-015.0*
sendmail	*CSSA-2003-016.0*

http://www.linuxsecurity.com/advisories/caldera.html

LINUX DEBIAN

Disponibilité de nombreux correctifs

Debian annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

bonsai	*DSA-265-1*
krb5	*DSA-266-1*
lpr	*DSA-267-1*
mutt	*DSA-268-1*
heimdal	*DSA-269-1*
kernel mips	*DSA-270-1*
ecartis	*DSA-271-1*
dietlibc	*DSA-272-1*
krb4	*DSA-273-1*
mutt	*DSA-274-1*
lpr ppd	*DSA-275-1*
kernel s390	*DSA-276-1*
apcupsd	*DSA-277-1*
sendmail	*DSA-278-1*
metrics	*DSA-279-1*
samba	*DSA-280-1*
moxftp	*DSA-281-1*
glibc	*DSA-282-1*
xfsdump	*DSA-283-1*
kdegraphics	*DSA-284-1*
lprng	*DSA-285-1*
gs-common	*DSA-286-1*
epic	*DSA-287-1*
openssl	*DSA-288-1*
rinetd	*DSA-289-1*
sendmail	*DSA-290-1*
ircii	*DSA-291-1*
mime support	*DSA-292-1*
kdelibs	*DSA-293-1*
gkrellm	*DSA-294-1*

http://www.debian.org/security/2003/



LINUX MANDRAKE

Disponibilité de nombreux correctifs

Mandrake annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

rxvt	*MDKSA-2003:034*	*8.2 / 9.0 / 9.1 / CS 2.1*
openssl	*MDKSA-2003:035*	*7.2 / 8.0 / 8.1 / 8 2 / 9.0 / 9.1 / FW 7.2 / FW 8.2 / CS 2.1*
netpbm	*MDKSA-2003:036*	*8 2 / 9.0 / 9.1 / FW 8.2 / CS 2.1*
glibc	*MDKSA-2003:037*	*7.2 / 8.0 / 8.1 / 8 2 / 9.0 / 9.1 / FW 7.2 / FW 8.2 / CS 2.1*
kernel	*MDKSA-2003:038*	*9.0 / CS 2.1*
kernel22	*MDKSA-2003:039*	*7.2 / 8.0 / 8.1 / 8 2 / FW 7.2*
Eterm	*MDKSA-2003:040*	*9.0*
mutt	*MDKSA-2003:041*	*8 2 / 9.0 / 9.1*
sendmail	*MDKSA-2003:042*	*8 2 / 9.0 / 9.1 / CS 2.1*
krb5	*MDKSA-2003:043*	*8 2 / 9.0 / 9.1 / FW 8.2 / CS 2.1*
samba	*MDKSA-2003:044*	*8 2 / 9.0 / 9.1 / FW 8.2 / CS 2.1*
evolution	*MDKSA-2003:045*	*9.0 / 9.1*
gtkhtml	*MDKSA-2003:046*	*9.1*
xfsdump	*MDKSA-2003:047*	*8 2 / 9.0 / 9.1 / CS 2.1*
eog	*MDKSA-2003:048*	*9.0 / 9.1 / CS 2.1*
kde3	*MDKSA-2003:049*	*9.0 / 9.1 / CS 2.1*
apache2	*MDKSA-2003:050*	*9.1*

http://www.linux-mandrake.com/en/security/

LINUX REDHAT

Disponibilité de nombreux correctifs

RedHat annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages :

glibc	*RHSA-2003:089-00*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0*
kernel22	*RHSA-2003:088-01*	*6.2 / 7.0*
evolution	*RHSA-2003:108-03*	*7.3 / 8.0*
samba	*RHSA-2003:095-03*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0 / 9.0*
kerberos	*RHSA-2003:051-01*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0*
sendmail	*RHSA-2003:120-01*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0*
dhcp	*RHSA-2003:034-01*	*8.0*
openssl	*RHSA-2003:101-01*	*6.2 / 7.0 / 7.1 / 7.2 / 7.3 / 8.0 / 9.0*
vsftpd	*RHSA-2003:084-01*	*9.0*
kerberos	*RHSA-2003:091-01*	*9.0*
eog	*RHSA-2003:128-01*	*8.0 / 9.0*
netpbm	*RHSA-2003:060-01*	*7.0 / 7.1 / 7.2 / 7.3 / 8.0*
balsa	*RHSA-2003:109-03*	*7.2 / 7.3 / 8.0 / 9.0*
samba	*RHSA-2003:137-02*	*7.1 / 7.2 / 7.3 / 8.0 / 9.0*
mgetty	*RHSA-2003:036-01*	*7.1 / 7.2 / 7.3 / 8.0*
kernel24	*RHSA-2003:135-00*	*9.0*
httpd	*RHSA-2003:139-01*	*8.0 / 9.0*
rhn	*RHSA-2003:080-01*	*8.0 / 9.0*
gtkhtml	*RHSA-2003:126-01*	*9.0*
tcpdump	*RHSA-2003:032-01*	*7.1 / 7.2 / 7.3 / 8.0*

http://www.linuxsecurity.com/advisories/redhat.html

MICROSOFT

Correctif pour le service d'indexation de NT 4.0

Microsoft a publié un correctif pour le service d'indexation de Windows NT 4.0, sujet à une vulnérabilité de type 'cross site scripting'. Microsoft [MS00-084]

http://www.microsoft.com/technet/security/bulletin/ms00-084.asp

Révision majeure de l'avis MS03-007

Microsoft a révisé son bulletin MS03-007 pour indiquer que la vulnérabilité présente dans 'ntdll.dll' et annoncée sur Windows 2000 affecte également Windows NT 4.0, bien que les codes d'exploitation existants soient inefficace contre ce système. Un correctif est disponible.

http://www.microsoft.com/technet/security/bulletin/MS03-007.asp

Correctif pour Windows 2000 et XP

Microsoft a publié les correctifs pour le service RPC de ses systèmes Windows 2000 et XP. Un utilisateur distant peut provoquer l'arrêt de ce service. Notons que cette alerte, initialement annoncée sur Windows 2000 a été étendue à Windows XP.

http://www.microsoft.com/technet/security/bulletin/MS03-010.asp



ORACLE

Révision de quatre alertes Oracle

Oracle a révisé quatre avis au sujet de plusieurs vulnérabilités affectant différentes versions de Oracle8, 8i et 9i Database. Cette mise à jour annonce la disponibilité de correctifs pour plusieurs plates-formes. Oracle

http://otn.oracle.com/deploy/security/pdf/2003alert51.pdf
http://otn.oracle.com/deploy/security/pdf/2003alert50.pdf
http://otn.oracle.com/deploy/security/pdf/2003alert49.pdf
http://otn.oracle.com/deploy/security/pdf/2003alert48.pdf

OpenBSD

Correctif pour Kerberos

OpenBSD a publié pour les systèmes OpenBSD 3.1 et 3.2, un correctif contre l'attaque cryptographique à laquelle sont vulnérables Kerberos 4 et 5. OpenBSD 'kerberos'

http://www.openbsd.org/errata.html#kerberos
http://www.openbsd.org/errata31.html#kerberos

Correctif pour Sendmail

OpenBSD a publié un correctif pour Sendmail, sujet à un débordement de buffer dans le traitement des en-têtes. OpenBSD 'sendmail'

ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/027_sendmail.patch
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.2/common/014_sendmail.patch

OpenSSH

Disponibilité de OpenSSH 3.6.1

Deux jours après la publication de OpenSSH 3.6, la version 3.6.1 est déjà disponible et corrige un bogue apporté par la version 3.6.

http://www.openssh.com/

SETI@home

Code d'exploitation pour la vulnérabilité SETI@home

Un code d'exploitation est disponible pour la vulnérabilité de type débordement de buffer affectant le logiciel de calcul du SETI.

http://safemode.org/files/zillion/exploits/seti-exploit.c

SGI

Vulnérabilités SNMP dans les commutateurs Brocade

SGI annonce que certains firmwares livrés avec les commutateurs Brocade sont vulnérables aux problèmes liés au protocole SNMP décrit dans le bulletin CERT CA-2002-03. Les versions inférieures à 2.6.0d sont vulnérables. Il n'existe pas de correctif et il est nécessaire d'installer la version 2.6.0d ou supérieure afin d'éliminer ces vulnérabilités

ftp://patches.sgi.com/support/free/security/advisories/20030405-01-I

Mise à jour des correctifs pour Tooltalk

SGI a mis à jour l'avis traitant de plusieurs vulnérabilités dans ToolTalk. Le nouveau correctif référencé 4915 permet d'éliminer toutes les failles décrites dans le bulletin CERT CA-1999.11. Les versions SGI 6.5.18 et 6.5.19 sont immunes à ces vulnérabilités.

ftp://patches.sgi.com/support/free/security/advisories/20021102-03-P

Correctif pour Sendmail

SGI a publié un correctif pour Sendmail, sujet à un débordement de buffer dans le traitement des en-têtes.

ftp://patches.sgi.com/support/free/security/advisories/20030401-01-P

SUN

Correctifs pour Sendmail

Sun a publié des correctifs pour Sendmail, sujet à un débordement de buffer dans le traitement des en-têtes. Ces correctifs sont disponibles pour Solaris 2.6 à 9, sur plates-formes Intel et Sparc.

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/52620

Révision de l'avis 27513 sur 'xview'

Sun a révisé l'avis 27513 au sujet d'un débordement de buffer dans la bibliothèque 'xview' pouvant être exploité afin d'acquérir localement des privilèges élevés. Cette révision indique que les correctifs pour Sun Solaris 2.6 (Sparc et Intel) sont désormais disponibles. Par ailleurs, l'avis étant clôt, il semble qu'aucun correctif ne sera fournit pour les autres plates-formes impactées.

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/27513

Correctifs pour 'priocntl' sur Solaris

Sun a publié l'ensemble des correctifs pour Solaris 2.6, 7, 8 et 9 résolvant la vulnérabilité affectant 'priocntl'. Notons que Solaris 2.5.1 nécessite une mise à jour vers une version plus récente du système.

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/49131



Correctifs pour NIS ('ypserv' et 'ypxfrd')
SUN a publié les correctifs pour les services 'ypserv' et 'ypxfrd' d'un serveur NIS pour Solaris 2.6, 7, 8 et 9. Notons que Solaris 2.5.1 nécessite une mise à jour du système et que Solaris 9 pour Intel n'est pas impacté.
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/47903

Correctifs pour Samba
Sun a publié pour Solaris 9 des correctifs pour Samba, vulnérable à un débordement de buffer exploitable à distance.
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/53580

Correctifs pour 'zlib'
Sun a publié de nouveaux correctifs pour la bibliothèque 'zlib'. Ces correctifs concernent l'environnement Gnome pour Solaris 8.
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F43541

Correctifs pour 'dtsession'
Sun a publié des correctifs pour les versions 2.6 à 8 de Solaris, concernant un débordement de buffer dans 'dtsession'. Désormais des correctifs pour les versions 2.6 à 9 de Solaris sont donc disponibles.
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/52388

Correctifs pour Sun ONE (iPlanet)
Sun a publié un avis concernant le débordement de buffer affectant le 'Connector Module' de Sun ONE. Celui-ci indique des correctifs pour la version 6.0 de Sun ONE. La version 6.5 est corrigée par l'application du Service Pack 1 ou de la Maintenance Update 3.
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/52022

Sun Linux et Cobalt affectés dans la fonction 'ptrace'
Sun a annoncé que sa distribution Sun Linux 5.0 (LX50) ainsi que les produits Sun Cobalt RaQ XTR, Qube3, RaQ4, CacheRaQ4(3100CR), RaQ550 et Control Station (SCCS) sont affectés par la vulnérabilité découverte dans la fonction 'ptrace' du noyau. Un utilisateur local peut exploiter cette faille afin d'obtenir les privilèges du compte 'root'. Les correctifs ou parades sont en attente et ne sont pas disponibles à ce jour.
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/52081

Correctif pour 'at'
Sun a publié un correctif pour Solaris 2.6 pour la commande 'at' qui permettait à un utilisateur local de détruire des fichiers du système.
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/50161

Correctifs pour 'cachefsd'
Sun a publié de nouveaux correctifs pour le service 'cachefsd', sujet à un débordement de buffer. Un correctif est désormais disponible pour chaque version de Solaris depuis la 2.5.1.
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert44309

CODES D'EXPLOITATION

Les codes d'exploitation des vulnérabilités suivantes ont fait l'objet d'une large diffusion :

LINUX

Disponibilité d'un code d'exploitation pour 'ptrace'
Un code d'exploitation pour la vulnérabilité affectant la fonction 'ptrace' du noyau de Linux est disponible sur le site Securiteam. Il permet à un utilisateur local d'acquérir les privilèges de 'root'.
http://www.securiteam.com/exploits/5CP0Q0U9FY.html

MICROSOFT

Disponibilité d'un code d'exploitation 'WebDAV'
Un code d'exploitation tirant parti du débordement de buffer présent dans la librairie 'ntdll.dll' et exploitable via la fonctionnalité 'WebDAV' IIS 5.0 a été diffusé hier soir sur de nombreuses listes de diffusion. L'étude rapide du code proposé montre que celui-ci tente d'exploiter la vulnérabilité via la requête WebDAV 'SEARCH' sur la cible dont on aura préalablement fourni l'adresse IP en paramètre. Si l'attaque fonctionne, une connexion offrant l'accès à l'interpréteur de commande est ouverte en retour sur le port TCP/666 du poste de l'attaquant (reverse remote shell). La mise à jour des systèmes vulnérables devient urgente.
http://rafa.h0stile.net/wbr.c – Source http://www.darksite.ch/edsa/coromputer/temp/wb.exe – Executable
http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0150.html

BULLETINS ET NOTES

Les bulletins d'information suivants ont été publiés par les organismes officiels de surveillance et les éditeurs :



CERT

Publication des statistiques au premier trimestre 2003

Le CERT a publié les statistiques relatives aux incidents et vulnérabilités ayant été traités au premier trimestre de l'année 2003. Le nombre d'incidents est de 42586 soit la moitié de toute l'année 2002, Le nombre de vulnérabilités est de 959 ce qui est stable depuis l'an passé, Le nombre d'alertes est en légère hausse avec 13 publications, Le nombre de notes de sécurité est en baisse avec 72 publications, Le nombre d'e-mails et d'appels traités sont tous deux largement en hausse.

http://www.cert.org/stats/cert_stats.html

Publication de la synthèse trimestrielle [CS-2003-01]

Le CERT publie, sous la référence CS-2003-01, la synthèse des mois de décembre 2002, janvier, février et mars 2003. Cette synthèse traite des vulnérabilités, exploitations ou attaques dont il a été question ces derniers mois :

1. *Débordement de buffer dans le noyau de Windows [CA-2003-09]*
2. *Débordement de buffer dans Sendmail [CA-2003-07]*
3. *Forte activité contre les partages de fichiers Windows [CA-2003-08]*
4. *Débordement de buffer dans Samba [VU#298233]*
5. *Apparition et propagation des vers Slammer et Sapphire [CA-2003-04] [CA-2002-22]*
6. *Vulnérabilités dans plusieurs implémentations de SIP [CA-2003-06]*
7. *Vulnérabilités dans plusieurs implémentations de SSH [CA-2002-36]*
8. *Débordement de buffer dans l'interface utilisateur de Windows [CA-2002-37]*
9. *Bogue 'double free' dans CVS [CA-2003-02]*
10. *Débordement de buffer dans le service 'locator' de Windows [CA-2003-03]*

Notons que ne sont pas évoqués les avis [CA-2003-01] et [CA-2003-05] portant respectivement sur le serveur DHCP de l'ISC et les serveurs Oracle. CERT/CC [CS-2003-01]

http://www.cert.org/summaries/CS-2003-01.html

SYMANTEC

Conseil d'écriture des règles de filtrage d'URL sur SEF

Suite à une alerte du site Corsaire, Symantec a publié une note indiquant comment utiliser les règles de filtrage d'URL de son pare-feu SEF (Symantec Enterprise Firewall) pour se protéger des URLs encodées à des fins de contournement de filtrage. Rappelons à ce propos que cette fonctionnalité est destinée à se protéger de l'emploi de caractères encodés dans un but de dissimulation, et non à effectuer un filtrage des pages accédées.

http://www.corsaire.com/advisories/030224-002.txt

http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2003032507434754

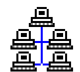


ATTAQUES

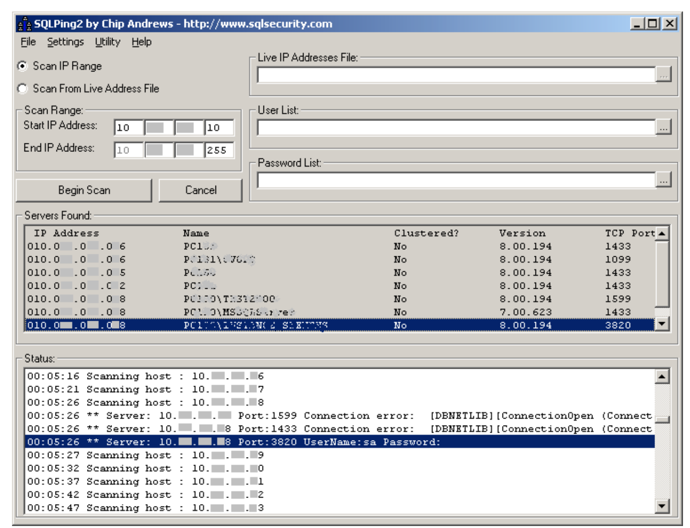
OUTILS

SQLPING.NET

▪ **Description**



L'utilitaire '**SQLPingV1.2**' développé par Chip Andrews facilite la recherche des serveurs sur lesquels le service '**SQL Server**' est actif. Cette version disponible depuis mai 2002 fonctionne en environnement WIN32.



Elle offre une interface graphique ergonomique permettant d'engager très rapidement un sondage.

Deux options fort utiles sont par ailleurs proposées:

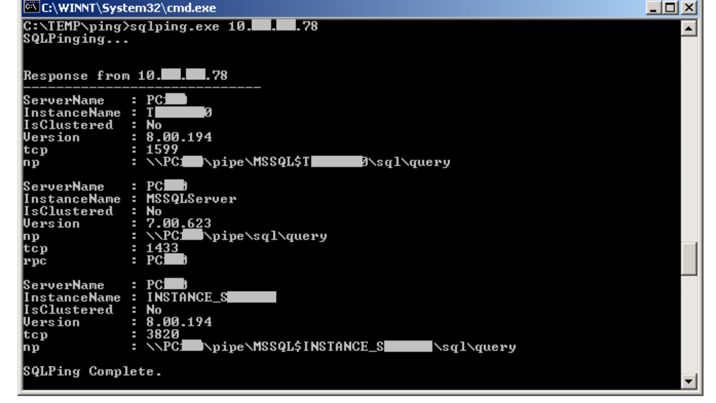
- Une recherche des systèmes SQL actifs par l'analyse de la réponse à une requête '**ICMP Echo**' – ou '**ping**' puis analyse de l'activité SQL,
- Le sondage forcé et systématique du port **TCP/1433** correspondant au point d'accès au service SQL Serveur.

L'utilisateur pourra s'il le souhaite indiquer comme adresse de départ, l'adresse IP de diffusion correspondant au réseau cible en lieu et place d'une plage d'adresses. Il sera ainsi possible d'identifier immédiatement les systèmes actifs et configurés pour répondre à une telle requête.

Cette méthode donne cependant des résultats généralement incomplets ou partiels conduisant à recommander de configurer le sondage en indiquant la plage des adresses IP cibles.

Une recherche systématique des comptes d'accès et mots de passe associés peut être activée en précisant le nom des fichiers contenant les identifiants et les mots de passe à tester. Dans l'hypothèse où aucun fichier n'est paramétré, l'outil recherchera simplement la présence d'un compte '**sa**' sans mot de passe, une situation hélas trop courante et exploitée avec grand bénéfice par de nombreux codes mobiles ou outils d'attaque.

Les tests menés sur cet outil ont prouvé son efficacité, le seul reproche qui puisse être formulé concerne la relative lenteur du sondage. Ainsi, le balayage de deux classes 'C' aura nécessité quelques 9mn avec une consommation conséquente des ressources du poste d'audit. Les résultats sont totalement satisfaisants car ayant permis de détecter un serveur dont l'une des trois instances d'une base SQL était configurée avec un compte '**sa**' sans mot de passe.



Une version allégée fonctionnant en mode 'ligne de commande' est disponible depuis le début de l'année. Développée autour de la technologie '**.NET**', cette version nécessite impérativement l'installation de la librairie '**MSCorEE.dll**' – Microsoft **C**omponent **o**bject **r**untime **E**xecution **E**ngine' – intégrée dans le paquetage '**.NET**'. Celui-ci devra en conséquence être installé sur le poste avec les éventuels risques que cela comporte, cette technologie étant encore très récente et comportant de nombreux 'bogues'.

A la différence de la version graphique, la version '**.NET**' n'autorise pas le sondage d'une plage d'adresse mais seulement l'analyse d'un système identifié par son adresse IP. Le principal intérêt de cette version – dont le code source est livré - est de pouvoir être utilisée dans un script.

▪ **Complément d'information**

http://www.sqlsecurity.com/uploads/sqlping22.zip

http://www.sqlsecurity.com/uploads/sqlping_dotnet.zip

TECHNIQUES

VIRUS ELF

▪ **Description**



Un manuel du '**parfait petit constructeur de virus UNIX**' a été publié sur l'Internet sous le titre '**The ELF Virus Writing HowTo**'. Nous nous proposons de fournir une synthèse des éléments fournis dans ce document en tenant compte des informations par ailleurs disponibles, notamment dans les excellents papiers écrits par **Silvio Cesare**.

Pour bien comprendre les mécanismes mis en œuvre dans l'écriture d'un virus d'une manière générale, et d'un virus UNIX infectant les objets **ELF** en particulier, il convient de faire quelques rappels ou compléments d'informations, sur ce qu'est un virus d'une part, et sur le format ELF lui même d'autre part.

Le Format ELF

Le format **ELF** (Executable and Linkable Format) a été conçu par les **U**nix **S**ystem **L**aboratories (USL) en tant que partie de l'Application Binary Interface. Ce format a été étudié pour faciliter le processus de développement, en proposant notamment la définition d'interfaces binaires valables sur plusieurs environnements. Un même code objet pourra ainsi être utilisé, c'est-à-dire chargé et exécuté, sur plusieurs systèmes UNIX d'origine différente. Le temps habituellement consacré au portage d'un code en est d'autant réduit.

A ce jour, le format '**ELF**' est utilisé par les fichiers objets ('**.o**'), des librairies partagées ('**.so**') et les exécutables. Il est reconnu par la majorité des systèmes UNIX, et dérivés, existants.

Notre propos étant de traiter de l'infection d'exécutables, nous nous attarderons plus particulièrement sur ce type de fichier que sur les fichiers objets ou les librairies partagées.

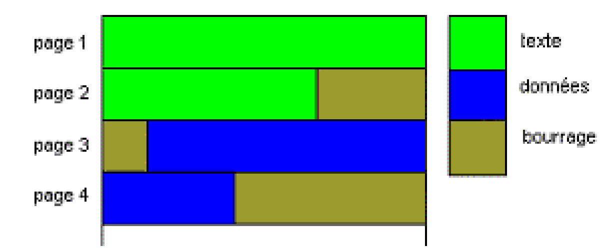
L'image d'un processus initié par un exécutable ELF contient au moins deux segments: un segment '**TEXT**' et un segment '**DATA**'. On notera que le segment texte peut être lu et exécuté, mais pas modifié en mémoire. Ceci empêchera par exemple l'utilisation de code se modifiant lui même dans la section '**TEXT**'.

La section '**DATA**' peut quant à elle être écrite et lue, mais pas exécutée.

Les segments de mémoire alloués à un processus ne sont en pratique jamais complètement utilisés, et l'espace restant est constitué de données sans autre utilité que d'assurer le remplissage ou 'bourrage' dans le jargon. Le segment '**DATA**' suit toujours le segment '**TEXT**'.

La représentation des pages mémoire allouées pour un processus proposée ci-contre permet de mieux visualiser l'organisation des données en mémoire.

Segment de mémoire alloué pour un processus



Dans un fichier exécutable **ELF** sont présents physiquement un certain nombre de segments à charger en mémoire, qui constitueront le segment '**DATA**' et le segment '**TEXT**' de l'image mémoire du processus. Plus précisément, un fichier exécutable ELF est constitué :

- d'une entête **ELF**
- de l'index de l'entête du programme
- des segments à charger en mémoire
- de l'index des sections optionnelles
- de segments optionnels (informations de débogage, …)

D'après les spécifications du format ELF, un fichier exécutable ELF commence par un entête qui contient une «carte» décrivant l'organisation du fichier. Les diverses sections contiennent, elles, diverses informations telles que des instructions, des données, une table de symboles, etc …

L'index de l'entête du programme, quand il existe, indique au système comment créer l'image du processus en mémoire. Cet index doit être présent dans un fichier exécutable pour qu'il soit valide. L'index des sections contient lui des informations sur les sections du fichier, comme leur nom, leur taille, etc…

Le fichier exécutable est une représentation « statique » du programme, et le système se charge d'en faire une représentation dynamique en mémoire via un programme spécifique dénommé 'loader' ou 'chargeur'. Cette représentation est composée des segments contenant le texte, les données, et la pile du processus.

Voyons, ci-dessous, la définition d'un entête ELF sur un système GNU/Linux :

```
/* The ELF file header.  This appears at the start of every ELF file.          */
typedef struct
{
  unsigned char   e_ident[EI_NIDENT];        /* Magic number and other info       */
  Elf32_Half      e_type;                    /* Object file type                  */
  Elf32_Half      e_machine;                 /* Architecture                      */
  Elf32_Word      e_version;                 /* Object file version               */
  Elf32_Addr      e_entry;                   /* Entry point virtual address       */
  Elf32_Off       e_phoff;                   /* Program header table file offset  */
  Elf32_Off       e_shoff;                   /* Section header table file offset  */
  Elf32_Word      e_flags;                   /* Processor-specific flags          */
  Elf32_Half      e_ehsize;                  /* ELF header size in bytes          */
  Elf32_Half      e_phentsize;               /* Program header table entry size   */
  Elf32_Half      e_phnum;                   /* Program header table entry count  */
  Elf32_Half      e_shentsize;               /* Section header table entry size   */
  Elf32_Half      e_shnum;                   /* Section header table entry count  */
  Elf32_Half      e_shstrndx;                /* Section header string table index */
} Elf32_Ehdr;
```

Nous porterons plus particulièrement notre attention sur les éléments suivants de la structure :

- '**e_entry**' est le point d'entrée du programme, donné sous forme d'adresse virtuelle,



- '**e_phoff**' donne l'adresse relative de l'index de l'entête du programme,
- '**e_shoff**' donne l'adresse relative de l'index de l'entête des sections.

Ce sont en effet ces éléments qui pourront être manipulés dans le cas d'une infection virale.

Voyons, maintenant la définition de l'entête du programme :

```
/* Program segment header.  */
typedef struct
{
  Elf32_Word      p_type;                   /* Segment type             */
  Elf32_Off       p_offset;                 /* Segment file offset      */
  Elf32_Addr      p_vaddr;                  /* Segment virtual address  */
  Elf32_Addr      p_paddr;                  /* Segment physical address */
  Elf32_Word      p_filesz;                 /* Segment size in file     */
  Elf32_Word      p_memsz;                  /* Segment size in memory   */
  Elf32_Word      p_flags;                  /* Segment flags            */
  Elf32_Word      p_align;                  /* Segment alignment        */
} Elf32_Phdr;
```

- '**p_type**' définit le type de segment. Dans le cas des segments chargeables du programme, qu'ils soient texte ou données, le type utilisé sera **PT_LOAD**.
- '**p_offset**' contient l'adresse relative du segment. Cet élément peut être manipulé dans le cas d'une infection virale.
- '**p_vaddr**' est l'adresse virtuelle du segment. Cette adresse peut être utilisée en adresse de base pour adresser de manière relative '**e_entry**',
- '**p_filesz**' et '**p_memsz**' sont respectivement la taille dans le fichier et la taille dans la mémoire occupées par le segment concerné. Ce mécanisme permet de réserver de l'espace mémoire quand il n'est pas forcément nécessaire pour charger le segment à partir du fichier.

Un des cas d'application de ce cas de figure est celui de la section '**.bss**' qui contient des données non initialisées à l'intérieur du segment de données. Il n'est en effet pas souhaitable d'occuper de l'espace dans le fichier avec des données non initialisées, mais le processus doit allouer suffisamment de mémoire. La section '**.bss**' se trouve à la fin du segment de données, et n'importe quelle valeur de '**p_memsz**' supérieure à '**p_filesz**' sera considérée comme faisant partie de '**.bss**'.

Voyons, enfin la définition d'une section :

```
/* Section header.  */
typedef struct
{
  Elf32_Word      sh_name;                  /* Section name (string tbl index)   */
  Elf32_Word      sh_type;                  /* Section type                      */
  Elf32_Word      sh_flags;                 /* Section flags                     */
  Elf32_Addr      sh_addr;                  /* Section virtual addr at execution */
  Elf32_Off       sh_offset;                /* Section file offset               */
  Elf32_Word      sh_size;                  /* Section size in bytes             */
  Elf32_Word      sh_link;                  /* Link to another section           */
  Elf32_Word      sh_info;                  /* Additional section information    */
  Elf32_Word      sh_addralign;             /* Section alignment                 */
  Elf32_Word      sh_entsize;               /* Entry size if section holds table */
} Elf32_Shdr;
```

L'élément ici important est '**sh_offset**', l'adresse relative de la section à l'intérieur du fichier.

Les virus

Le concept de virus est souvent utilisée à tort, voir confondu avec le concept de vers ou de cheval de Troie.

- Un virus est un programme qui cherche à infecter les représentations statiques d'autres programmes. Le terme représentation statique est utilisé par opposition à l'image en mémoire d'un processus, et représente donc la forme du fichier exécutable du programme.
- Un ver est un programme qui exploite les vulnérabilités d'autres programmes. Une copie du code du ver est alors effectuée dans la mémoire du processus infecté.
- Un cheval de Troie est un programme destiné à être lancé par un utilisateur naïf, présentant un aspect anondin, et effectuant des tâches à l'insu de l'utilisateur.

L'infection de fichiers ELF

L'insertion de code parasite dans un fichier ELF nécessite que le chargement de l'image du processus se fasse de manière à ce que le code et les données d'origines restent intacts. Cela nécessite donc que la mémoire allouée pour les segments soit plus grande.

Une modification du segment de texte impacterait l'entête ELF, mais aussi les informations nécessaires à l'édition dynamique des liens par le chargeur. L'insertion d'un segment est parfaitement réalisable mais peu discrète. L'utilisation des zones vierges aux extrémités des segments semble être la meilleure solution pour garantir l'intégrité du code et des données du programme original tout en palliant aux problèmes de détection. Le choix se portera naturellement sur la zone de remplissage localisée à la suite de la section texte.

Il est possible d'agrandir le segment '**TEXT**'vers le bas et en conséquence la place disponible dans la zone de remplissage avant la section de données. Par contre, agrandir le segment '**TEXT**' vers le haut, ou le segment '**DATA**' vers le bas risque d'entraîner des recouvrements avec d'autres segments.

Nous allons détailler deux types d'infection de fichier **ELF** exécutable :



- L'infection par ajout de segment
- L'infection par utilisation d'une zone de remplissage

Infection par ajout de segment

Cette méthode est, nous l'avons déjà dit, simple à mettre en œuvre, mais également très facile à repérer. L'entête **ELF** contient le champ '**e_machine**' permettant de différencier l'architecture mais pas le système d'exploitation. Cette différentiation est effectuée par le biais d'une autre entête de programme de type **PT_NOTE**. Lorsque cette section est manquante, l'exécutable sera considéré comme natif et la compatibilité binaire ne pourra être exploitée. Un exécutable '**Linux**' infecté ne pourra être lancé par un système '**FreeBSD**'.

Concrètement, l'infection est effectuée en deux étapes :

- Ecrasement de l'entête de programme de type **PT_NOTE** avec une définition de segment de code de type **LOAD**,
- Ajout du code viral à la fin du fichier exécutable.

On remarquera qu'une double infection du même fichier exécutable n'est pas possible, étant donné qu'il ne peut exister qu'une seule entête de type **PT_NOTE**.

Le gros désavantage de cette méthode est qu'elle est très facilement détectable. Elle conduit à un binaire infecté dont la taille sera supérieure à celle de l'original et écrase le contenu d'une entête '**ELF**'. Il suffira à un outil de détection d'analyser l'en-tête de type **PT_NOTE** pour détecter l'infection.

Infection d'une zone de remplissage

Cette seconde méthode d'infection a beaucoup fait parler d'elle à l'occasion de la diffusion du célèbre cheval de Troie '**Remote Shell Trojan**' dit '**RST**', premier code connu à utiliser cette méthode. Lez segment '**TEXT**' et '**DATA**' peuvent être infectés. Toutefois, l'infection du segment '**DATA**' implique quelques contraintes, notamment le fait que celui ci soit exécutable.

L'infection d'une zone de remplissage dans le segment de texte nécessite plusieurs actions :

- augmenter la valeur du champ '**e_shoff**' pour tenir compte du nouveau code dans l'entête ELF,
- trouver l'entête de programme du segment de texte et modifier '**p_filesz**' et '**p_memsz**' pour tenir compte du nouveau code dans l'entête,
- pour chaque entête de programme dont le segment se trouve après le segment de texte infecté, modifier '**p_offset**' pour indiquer la nouvelle position,
- pour chaque entête de section se trouvant après l'insertion, augmenter '**sh_offset**' pour tenir compte du nouveau code,
- rajouter physiquement le code dans le fichier dans le segment de texte se trouvant à l'adresse '**p_offset**' + '**p_filesz**' (avant modification).

Nous rencontrons toutefois un léger problème. En effet la spécification du format '**ELF**' précise que '**p_vaddr**' et '**p_offset**' doivent être congruents modulo la taille d'une page (définie par **PAGE_SIZE**). Cela veut dire que n'importe quelle insertion de données dans le segment '**TEXT**' devra être congruente modulo la taille d'une page. La taille du segment '**TEXT**' n'aura cependant pas à être modifiée. Cette manipulation induit l'effet de bord suivant: une page complète de mémoire devra être utilisée comme zone de remplissage car l'adresse '**vaddr**' requise n'est pas disponible. Cet effet de bord aura pour conséquence d'offrir au code parasite plus de place pour s'insérer. L'allocation de la page requise n'est cependant pas toujours garantie.

L'algorithme précédent sera donc modifié pour tenir compte de la contrainte de congruence entre '**p_offset**' et '**p_vaddr**':

- augmenter la valeur de '**e_shoff**' de **PAGE_SIZE** dans l'entête ELF,
- modifier le code viral pour qu'il effectue un saut sur le point d'entrée original du binaire infecté,
- localiser le segment '**TEXT**' infecté,
- modifier le point d'entrée de l'entête ELF pour pointer sur le code viral ('p_vaddr' + 'p_filesz'),
- modifier '**p_filesz**' et '**p_memsz**' pour tenir compte du code inséré,
- pour chaque segment '**TEXT**' se trouvant après le segment '**TEXT**' infecté, incrémenter '**p_offset**' de PAGE_SIZE
- pour chaque entête de section se trouvant après l'insertion, augmenter '**sh_offset**' de PAGE_SIZE,
- enfin, copier physiquement le code dans le segment de texte se trouvant à l'adresse 'p_offset' + 'p_filesz' (avant modification) et compléter à concurrence de PAGE_SIZE par un remplissage.

Bien que totalement fonctionnel, cet algorithme ne tient pas compte du fait que le code ajouté dans le segment '**TEXT**' ne corresponde à aucune section déclarée. Il faudra donc modifier l'entête de section pour que celle-ci intègre le code viral dans la taille du segment déclaré via la variable '**sh_len**'.

L'algorithme précédent devient donc :

- augmenter la valeur de '**e_shoff**' de **PAGE_SIZE** dans l'entête ELF,
- modifier le code viral pour qu'il effectue un saut sur le point d'entrée original du binaire infecté,
- localiser le segment '**TEXT**' infecté,
- modifier le point d'entrée de l'entête ELF pour pointer sur le code viral ('**p_vaddr**' + '**p_filesz**'),
- modifier '**p_filesz**' et '**p_memsz**' pour tenir compte du code inséré,
- pour chaque segment '**TEXT**' se trouvant après le segment '**TEXT**' infecté, incrémenter '**p_offset**' de PAGE_SIZE
- modifier '**sh_len**' dans la dernière entête de section du segment 'TEXT' infecté en ajoutant la taille du code viral,
- pour chaque entête de section se trouvant après l'insertion, augmenter '**sh_offset**' de PAGE_SIZE,
- enfin, copier physiquement le code dans le segment de texte se trouvant à l'adresse 'p_offset' + 'p_filesz' (avant modification) et compléter à concurrence de PAGE_SIZE par un remplissage.



Cette méthode d'infection est doublement intéressante puisque le virus n'infectera un fichier qu'à la condition de disposer de la place nécessaire pour s'insérer et qu'un même exécutable pourra être infecté par différents codes, ceux-ci étant par construction chaînés les uns aux autres, le code orignal étant exécuté en dernier.

Le lecteur retiendra de cette synthèse (dont nous devons avouer qu'elle reste très technique) l'apparition d'un phénomène assez nouveau dans la communauté des auteurs de codes mobiles, celui de la mise en œuvre d'une approche méthodologique de plus en plus rigoureuse conduisant à la découverte de procédés d'infection 'génériques', et donc à la diffusion d'un mode opératoire précis et aisément mis en œuvre.

- **Complément d'information**

http://virus.enemy.org/virus-writing-HOWTO/_html/	Le manuel du parfait auteur de virus
http://www.big.net.au/~silvio	Une référence en matière de travaux sur l'exploitation du format ELF
http://s2.enemy.org/~alba/SilvioCesare/	Divers travaux portant sur l'écriture de codes mobiles

IRC BotNet - Scan of The Month

- **Description**

Proposé par les membres du projet '**HoneyNet**' de l'université d'**Azuza**, le défi du mois d'avril vise à analyser les multiples attaques subies par un pot de miel basé sur un système Windows 2000. Début mars 2003, un Windows 2000 a en effet été installé sur le réseau Internet sans qu'aucun mot de passe n'ait été configuré pour le compte administrateur. Durant les premières semaines de l'installation, cette machine a régulièrement été compromise aussi bien par des pirates que par des codes mobiles. A la suite d'une attaque réussie, la machine a été intégrée dans un réseau IRC automatisé ou '**botnet**'. Durant la période d'activation du système, plus de 15164 systèmes ont utilisé ce point d'entrée sur le réseau.

L'objectif du défi est d'analyser les évènements collectés par une sonde 'snort' durant une période de 5 jours et de répondre aux questions suivantes organisées par niveau de difficulté.

Niveau débutant

1. *Qu'est ce que IRC ?*
2. *Quel est le message transmis par IRC pour rejoindre le réseau ?*
3. *Qu'est ce qu'un '**botnet**' ?*
4. *Quelle est généralement l'utilité d'un 'botnet' ?*
5. *Quels sont les ports couramment utilisés par **IRC** ?*
6. *Qu'est ce qu'un fichier de journalisation binaire et comment est-il créé ?*
7. *Avec quels serveurs IRC le système compromis, dont l'adresse est 172.16.134.191, communique-t-il ?*
8. *Sur la période d'analyse, combien de systèmes distincts ont accédé le botnet via le serveur 209.196.44.172 ?*
9. *En considérant que chaque nœud du botnet dispose d'un lien de 56Kps, quelle est la bande passante du botnet ?*

Niveau intermédiaire

1. *Quelles sont les adresses IP sources utilisées pour attaquer le pot de miel ?*
2. *Quelles vulnérabilités les attaquants ont-ils tenté d'exploiter ?*
3. *Quelles ont été les attaques réussies ?*

Préparation de l'environnement

La première étape consiste à préparer l'environnement d'analyse sur nos systèmes **LINUX** et **Windows**. Nous utiliserons principalement les outils '**Ethereal**' dans sa version **0.9.11** et '**snort**' dans sa distribution **1.9.1**.

Validation du fichier livré

Le fichier '**sotm27.zip**' d'une taille de 13Mo contient les journaux générés par '**snort**' au format dit 'binaire'. Un rapide contrôle de la somme cryptographique '**MD5**' du fichier '**.zip**' permet de s'assurer de l'intégrité de la distribution, ici:

```
C:> md5 sotm27.zip
     868a97c642f926630b9e20ce5024a251
```

à comparer avec la somme donnée sur le site du défi :

```
MD5 (sotm27.gz) = 868a97c642f926630b9e20ce5024a251
```

L'intégrité de l'archive téléchargée est confirmée – du moins en considérant que la somme de contrôle annoncée sur le site n'a pas aussi été manipulée. La décompression de l'archive nous livre le fichier de travail d'un volume de 18Mo.

Etude des données journalisées

Le fichier '**sotm27**' contient quelques **18Mo** de données journalisées au format dit '**tcpdump**'. Deux approches peuvent être employées pour étudier celles-ci:

1. Analyse manuelle à l'aide des outils '**ethereal**', '**tcpdump**', '**tcptrace**' et '**tcpflow**'
2. Analyse semi-automatique à l'aide de l'outil '**Snort**'

Etant donné le volume de données à analyser, nous allons procéder en trois étapes:

- acquisition d'éléments statistiques par le biais des outils '**ethereal**' et '**tcpdump**',
- étude des attaques en s'appuyant sur '**tcpflow**' et '**snort**'
- et enfin, si besoin, étude détaillée de certains paquets sous '**Ethereal**'.

Obtention d'éléments statistiques



Le chargement du fichier '**sotm27**' sous '**Ethereal**' nous permet d'obtenir les informations suivantes sur le contexte:

- Quelques **54536** paquets ont été journalisés entre le 1 mars 2003 à 10h08 et le 6 mars à 9h27.
- La fonction d'analyse statistique présente sous '**Ethereal**' nous permet d'établir une liste des protocoles présentés triés par activité:

Protocole / Service		Nb. Paquets	Soit en %
TCP		54350	99,66
	HTTP	12028	22,07
	IRC	9809	17,99
	NetBIOS Session	3769	6,91
	DATA	918	1,68
	SSL	1	0,00
UDP		186	0.34
	NetBIOS Name Svc	129	0,24
	DEC RPC	55	0,10
	DATA	2	0,00

Cette rapide étude met en évidence la prépondérance de l'utilisation des protocoles TCP '**HTTP**', '**IRC**' puis '**NetBIOS**'. Le positionnement d'un filtre '**ip.addr eq 172.16.134.191**' permet de confirmer que les évènements journalisés concernent tous le système compromis dont l'adresse '**172.16.134.191**' nous est donnée dans la présentation du défi.

Protocole TCP

L'utilisation de l'excellent utilitaire '**tcpdump**' va nous permettre d'extraire rapidement tous les échanges **TCP** ayant été journalisés et ainsi d'obtenir une liste exhaustive des adresses IP des systèmes ayant communiqués avec la cible. On notera en effet que la liste d'adresses IP produites par l'outil '**snort**' est généralement restreinte aux seules adresses ayant déclenchées l'une des règles d'analyse.

Le script suivant va nous permettre d'extraire automatiquement les informations nécessaires: adresse IP source, port destination ainsi que l'activité mesurée en terme de nombre de sessions engagées.

```
tcpdump -n -nn -r ../sotm27 'dst 172.16.134.191 and tcp[13] =2' | \    Paquets SYN uniquement
awk '{print $3 " " $5;}' | \                                           Source et Destination
awk -F'.' '{print $9 "\t" $1 "." $2 "." $3 "." $4;}' |\                Adresse Src, Port Dst
sed -e 's/://' | \                                                     Nettoyage
sort | \                                                               Tri par adresse
uniq –c –1 | \                                                         Comptage tentatives
awk '{print $3 "\t" $2 "\t" $1;}' | \                                  Réordonnancement
sort > resultats.txt                                                   Tri sur adresse
```

Les différents éléments ainsi obtenus sont récapitulés dans le tableau suivant qui met en évidence 2 systèmes particulièrement actifs sur les **77** sources **TCP** répertoriées. On notera par ailleurs la nette prédominance du service **NetBios Session Service** (**TCP/139**) en tant que cible d'une session ou tentative d'ouverture de session.

Connexions TCP sur la cible			
Adresse	**Nom DNS**	**Services accédés**	**Cnx**
24.197.194.106	24-197-194-106.man.mn.charter.com	…80,110,111,139,1433	1229
210.22.204.101		80,99,139,445,1433,….	105
129.116.182.239	dhcp-129-116-182-239.fsel.utexas.edu	57,139,445,1433	10
66.139.10.15	adsl-66-139-10-15.dsl.hstntx.swbell.net	139,445	6
209.45.125.69		139,445	6
61.111.101.78		139,445	5
195.36.247.77	f01m-8-77.d3.club-internet.fr	135,139,445	5
192.215.160.106		1433	4
172.168.0.154	aca8009a.ipt.aol.com	139	4
213.23.49.158	dsl-213-023-049-158.arcor-ip.net	57,80	4
192.130.71.66		57,80	4
194.199.201.9	uc9.marnelavallee.archi.fr	1433	3
80.181.116.202	host202-116.pool80181.interbusiness.it	139,445	3
66.8.163.125	a66b8n163client125.hawaii.rr.com	80,139,445	3
209.45.125.110		139	3
216.170.214.226		139	2
213.84.75.42	213-84-75-42.adsl.xs4all.nl	139	2
210.111.56.66		1433	1
200.74.26.73	pc-200-74-26-73.las-condes4.pc.metropolis-inter.com	1080	1
81.50.177.167	amarseille-206-1-19-167.abo.wanadoo.fr	139	1
81.202.125.5	81-202-125-5.user.ono.com	139	1
68.154.11.82	adsl-154-11-82.asm.bellsouth.net	139	1
68.152.53.138		139	1
68.115.33.110	c68.115.33.110.mazo.wi.charter.com	139	1
66.73.160.240	adsl-66-73-160-240.dsl.chcgil.ameritech.net	139	1
66.190.67.122	c66.190.67.122.ts46v-16.otn-h2.ftwrth.tx.charter.com	139	1



64.254.203.68	ip-203-68.theramp.net	139	1
64.17.250.240	cable6-240.fctvplus.net	139	1
62.251.129.118		139	1
62.201.96.159	adsl-159-96.adsl-pool.axelero.hu	139	1
62.194.4.114	node-c-0472.a2000.nl	139	1
61.55.71.169		139	1
61.177.154.228		139	1
61.155.126.150		139	1
61.140.149.137		139	1
61.14.66.92		139	1
4.64.221.42	washdc3-ar2-4-64-221-042.washdc3.elnk.dsl.genuity.net	139	1
24.161.196.103	bak-24-161-196-103.bak.rr.com	139	1
219.94.46.57		139	1
219.118.31.42	db761f2a.speednet.ne.jp	139	1
218.87.178.167		139	1
218.237.70.119		139	1
218.163.9.89	218-163-9-89.HINET-IP.hinet.net	139	1
217.227.98.82	pd9e36252.dip.t-dialin.net	139	1
217.227.245.101	pd9e3f565.dip.t-dialin.net	139	1
217.222.201.82	host82-201.pool217222.interbusiness.it	139	1
217.1.35.169	pd90123a9.dip.t-dialin.net	139	1
213.7.60.57	b3c39.pppool.de	139	1
213.44.104.92	lven2-5-92.n.club-internet.fr	139	1
213.217.55.243		139	1
213.116.166.126	1cust126.tnt36.rtm1.nld.da.uu.net	139	1
213.107.105.72	pc2-cmbg1-4-cust72.cmbg.cable.ntl.com	139	1
212.110.30.110		139	1
210.58.0.25	25.c0.ethome.net.tw	139	1
210.214.49.227	dialpool-210-214-49-227.maa.sify.net	139	1
210.203.189.77	ipnet77-p2.anet.net.th	139	1
210.12.211.121		139	1
208.186.61.2	208-186-61-2.nrp3feld.roc.ny.frontiernet.net	139	1
207.6.77.235	a0iu57esy46i9.bc.hsia.telus.net	139	1
203.115.96.146		139	1
202.63.162.34	202-63-162-34.exatt.com	139	1
200.78.103.67	dsl-200-78-103-67.prodigy.net.mx	139	1
200.66.98.107		139	1
200.60.202.74	client-200.60.202.74.speedy.net.pe	139	1
195.67.251.197	t6o37p17.telia.com	139	1
169.254.205.177		139	1
168.226.98.61	168-226-98-61.speedy.com.ar	139	1
164.125.76.48		139	1
162.33.189.252		139	1
144.134.109.25	drpp-p-144-134-109-25.prem.tmns.net.au	139	1
141.149.155.249	pool-141-149-155-249.buff.east.verizon.net	139	1
212.243.23.179		111	1
204.50.186.37		111	1
68.169.174.108	ca-lahabra-cuda1-c6b-108.anhmca.adelphia.net	80	2
218.25.147.83		80	1
203.170.177.8		21	3
141.85.37.78		21	1

Le script précédent légèrement modifié nous permettra d'obtenir aussi aisément la liste des systèmes vers lesquels la cible a tenté d'initialiser une session TCP.

```
tcpdump -n -nn -r ../sotm27 'src 172.16.134.191 and tcp[13] =2' | \   Paquets SYN uniquement
awk '{print $3 " " $5;}' | \                                          Source et Destination
awk -F'.' '{print $9 "\t" $5 "." $6 "." $7 "." $8;}' | \              Adresse Src, Port Dst
sed -e 's/://' | \                                                    Nettoyage
awk '{print $1 "\t" $3;}' | \                                         Réorganisation
sort | \                                                              Tri par adresse
uniq –c –1 | \                                                        Comptage tentatives
awk '{print $3 "\t" $2 "\t" $1;}' | \                                 Ré ordonnancement
sort > resultats.txt                                                  Tri sur adresse
```

Cette liste est pour le moins réduite : 32 systèmes avec une majorité de connexions vers un serveur WEB (port 80), les deux autres services contactés correspondant au service **IRC** (**TCP/6667**) et à une porte dérobée de type **BackOrifice** (**TCP/31337**)

Connexions TCP depuis la cible			
Adresse	Nom DNS	Services accédés	Cnx



199.107.7.2		**31337**	3
209.126.161.29		**6667**	9
66.33.65.58	ns.espaciosweb.net	**6667**	9
209.196.44.172	ipdwbc0271atl2.public.registeredsite.com	**6667**	1
217.199.175.10	ns2.caralarmuk.com	**6667**	1
63.241.174.144		**6667**	1
216.154.242.126		80	6
128.242.214.10		80	4
207.172.16.156	www.rcn.com	80	4
207.68.171.238	msimg.com	80	4
207.172.16.150	users.mrf.va.web.rcn.net	80	3
217.140.0.47		80	3
194.68.68.39		80	2
205.188.137.80	streamer013.cache. aol.com	80	2
207.46.196.108	activex.microsoft.com	80	2
207.68.176.250	auto.search.msn.com	80	2
216.239.33.101	www.google.com	80	2
216.239.51.100	www.google.com	80	2
217.151.192.226	www.torget.se	80	2
217.151.192.231	spel.torget.se	80	2
194.192.187.194		80	1
194.68.68.12		80	1
198.49.161.200	crl-brun1.verisign.com	80	1
206.151.167.254		80	1
207.46.196.120	codecs.microsoft.com	80	1
207.68.171.245	www.msn.com	80	1
207.68.183.190	passportimages.com	80	1
207.68.184.62		80	1
213.66.244.241	d1o809.telia.com	80	1
216.239.57.100	www.google.com	80	1
64.0.96.9		80	1
65.57.83.13	download.macromedia.com	80	1

Les éléments ainsi collectés vont nous permettre de cibler notre analyse.

Protocole UDP

La liste des **113** systèmes ayant transmis un paquet **UDP** à destination de la cible est obtenue à l'aide d'un nouveau script inspiré des précédents. Les services accédés correspondent majoritairement au service **Netbios Name Service** (**UDP/137**) et au désormais célèbre **Microsoft SQL Monitor** (**UDP/1434**) exploité par le ver '**SQL-Slammer**'.

Connexions UDP vers la cible			
Adresse	**Nom DNS**	**Services accédés**	**Cnx**
61.150.72.7		1434	4
61.132.88.90	TC2-27.wx.js.cn	1434	3
61.150.120.72		1434	2
61.134.45.19		1434	2
24.197.194.106	24-197-194-106.man.mn.charter.com	137	2
218.4.99.237		1434	2
62.150.170.232		28431	1
62.150.170.134		28431	1
81.57.217.208	lns-th2-2-81-57-217-208.adsl.proxad.net	1434	1
68.84.210.227	pcp02606068pcs.prtmry01.nj.comcast.net	1434	1
68.45.123.130	pcp099250pcs.glstrt01.nj.comcast.net	1434	1
68.37.54.69	bgp453726bgs.avenel01.nj.comcast.net	1434	1
67.81.161.166	ool-4351a1a6.dyn.optonline.net	1434	1
67.201.75.38	1Cust38.tnt2.york.pa.da.uu.net	1434	1
66.81.131.17	host-66-81-131-17.rev.o1.com	1434	1
66.233.4.225	cdm-66-4-225-bnvl.cox-internet.com	1434	1
61.8.1.64	ppp64.dyn1.pacific.net.au	1434	1
61.203.104.148	IP1A1352.hkd.mesh.ad.jp	1434	1
61.185.29.9		1434	1
61.185.242.190		1434	1
61.185.215.42		1434	1
61.185.212.166		1434	1
61.177.62.66		1434	1
61.177.56.98		1434	1
61.132.88.50	TC1-50.wx.js.cn	1434	1
4.33.244.44	lsanca2-ar31-4-33-244-044.lsanca2.dsl-verizon.net	1434	1
24.74.199.104	cae74-199-104.sc.rr.com	1434	1



24.167.221.106	CPE-24-167-221-106.wi.rr.com	1434	1
219.145.211.3		1434	1
219.145.211.132		1434	1
218.92.13.142		1434	1
218.4.87.137		1434	1
218.4.65.115		1434	1
218.4.48.74		1434	1
218.244.66.32		1434	1
217.35.65.9	host217-35-65-9.in-addr.btopenworld.com	1434	1
216.229.73.11	216-229-73-11-empty.fidnet.com	1434	1
216.192.145.21	chi-tgn-gjj-vty21.as.wcom.net	1434	1
213.170.56.83		1434	1
213.122.77.74	host213-122-77-74.in-addr.btopenworld.com	1434	1
212.162.165.18	212-162-165-18.skbbip.com	1434	1
212.122.20.74	dsl-20-074.primorye.ru	1434	1
206.149.148.192	192-pool1.ras10.vaash.alerondial.net	1434	1
200.50.124.2	50-124-2.leased.cust.tie.cl	1434	1
200.135.228.10	free228010.unidavi.rct-sc.br	1434	1
168.243.103.205		1434	1
12.83.147.97	97.omaha-02rh16rt.ne.dial-access.att.net	1434	1
12.253.142.87	12-253-142-87.client.attbi.com	1434	1
12.252.61.161	12-252-61-161.client.attbi.com	1434	1
205.180.159.35		1434	1
81.50.177.167	amarseille-206-1-19-167.abo.wanadoo.fr	137	1
81.202.125.5	81-202-125-5.user.ono.com	137	1
81.114.77.37	host37-77.pool81114.interbusiness.it	137	1
68.154.11.82	adsl-154-11-82.asm.bellsouth.net	137	1
68.152.53.138		137	1
68.115.33.110	c68.115.33.110.mazo.wi.charter.com	137	1
66.92.135.108	dsl092-135-108.chi1.dsl.speakeasy.net	137	1
66.73.160.240	adsl-66-73-160-240.dsl.chcgil.ameritech.net	137	1
66.190.67.122	c66.190.67.122.ts46v-16.otn-h2.ftwrth.tx.charter.com	137	1
64.254.203.68	ip-203-68.theramp.net	137	1
64.17.250.240	cable6-240.fctvplus.net	137	1
62.251.129.118		137	1
62.201.96.159	adsl-159-96.adsl-pool.axelero.hu	137	1
62.194.4.114	node-c-0472.a2000.nl	137	1
62.127.38.198	du-38-198.ppp.telenordia.se	137	1
61.55.71.169		137	1
61.177.154.228		137	1
61.155.126.150		137	1
61.140.149.137		137	1
61.14.66.92		137	1
61.11.11.54		137	1
4.64.221.42	washdc3-ar2-4-64-221-042.washdc3.elnk.dsl.genuity.net	137	1
24.161.196.103	bak-24-161-196-103.bak.rr.com	137	1
24.107.117.237	commons10k1.mo24.107.117.237.charter-stl.com	137	1
219.94.46.57		137	1
219.65.37.37	PPP-219.65.37.37.mum2.vsnl.net.in	137	1
219.118.31.42	db761f2a.speednet.ne.jp	137	1
218.87.178.167		137	1
218.237.70.119		137	1
218.163.9.89	218-163-9-89.HINET-IP.hinet.net	137	1
217.227.98.82	pd9e36252.dip.t-dialin.net	137	1
217.227.245.101	pd9e3f565.dip.t-dialin.net	137	1
217.222.201.82	host82-201.pool217222.interbusiness.it	137	1
217.1.35.169	pd90123a9.dip.t-dialin.net	137	1
216.228.8.158	216-228-8-158.dsl.redshift.com	137	1
216.170.214.226		137	1
213.84.75.42	213-84-75-42.adsl.xs4all.nl	137	1
213.7.60.57	b3c39.pppool.de	137	1
213.44.104.92	lven2-5-92.n.club-internet.fr	137	1
213.217.55.243		137	1
213.116.166.126	1Cust126.tnt36.rtm1.nld.da.uu.net	137	1
213.107.105.72	pc2-cmbg1-4-cust72.cmbg.cable.ntl.com	137	1
212.110.30.110		137	1
211.149.57.197		137	1
210.58.0.25	25.c0.ethome.net.tw	137	1



210.214.49.227	dialpool-210-214-49-227.maa.sify.net	137	1
210.203.189.77	ipnet77-p2.anet.net.th	137	1
210.12.211.121		137	1
208.186.61.2	208-186-61-2.nrp3feld.roc.ny.frontiernet.net	137	1
207.6.77.235	a0iu57esy46i9.bc.hsia.telus.net	137	1
203.115.96.146		137	1
203.106.55.12		137	1
202.63.162.34		137	1
200.78.103.67	202-63-162-34.exatt.com	137	1
200.66.98.107	dsl-200-78-103-67.prodigy.net.mx	137	1
200.60.202.74	client-200.60.202.74.speedy.net.pe	137	1
195.67.251.197	t6o37p17.telia.com	137	1
168.226.98.61	168-226-98-61.speedy.com.ar	137	1
164.125.76.48		137	1
162.33.189.252		137	1
148.235.82.146	customer-148-235-82-146.uninet.net.mx	137	1
144.134.109.25	drpp-p-144-134-109-25.prem.tmns.net.au	137	1
141.149.155.249	pool-141-149-155-249.buff.east.verizon.net	137	1

L'étude des paquets **UDP** transmis depuis la cible à destination des systèmes tiers montre qu'ils correspondent tous à une réponse aux requêtes émises vers le port '**UDP/137**'.

Utilisation de 'tcptrace'

Nous avons volontairement choisi d'analyser les événements journalisés par l'intermédiaire de scripts écrits sur mesure qui, si nous étions dans un environnement d'exploitation auraient fait l'objet d'améliorations afin de générer automatiquement toutes les informations nécessaires, ceci probablement dans un format similaire à celui utilisé par le remarquable outil d'analyse '**fwlogwatch**'. On notera à ce propos qu'il est fort dommage que ce dernier ne reconnaisse pas le format '**tcpdump**' parmi les quelques 10 formats connus: **cisco**, **netscreen**, **snort text**, …

Un outil du domaine public, '**tcptrace**' permet d'engager une analyse assez similaire à la notre en proposant une présentation des évènements journalisés plus lisible que la présentation native de l'outil '**tcpdump**'. Ainsi la commande suivante nous générera une synthèse de toutes les connexions **TCP** journalisées:

```
# tcptrace –b sotm27
 1 arg remaining, starting with 'sotm27'
 Ostermann's tcptrace -- version 6.2.0 -- Fri Jul 26, 20
 54536 packets seen, 54350 TCP packets traced
 elapsed wallclock time: 0:02:45.367537, 329 pkts/sec analyzed
 trace file elapsed time: 119:19:48.341961
 TCP connection info:
    1: db761f2a.speednet.ne.jp:2388            - 172.16.134.191:139       (a2b)     4>    3<   (reset)
    2: 218-163-9-89.HINET-IP.hinet.net:4760    - 172.16.134.191:139       (c2d)     2>    1<
    3: dsl-213-023-049-158.arcor-ip.net:1445   - 172.16.134.191:80        (e2f)     6>    5<   (complete)
    4: dsl-213-023-049-158.arcor-ip.net:1490   - 172.16.134.191:57        (g2h)     3>    3<   (reset)
    5: 61.155.126.150:1716                     - 172.16.134.191:139       (i2j)     4>    3<   (reset)
    6: 210.111.56.66:1929                      - 172.16.134.191:1433      (k2l)     1>    1<   (reset)
 …
1743: 172.16.134.191:1152                     - 271atl2.registered.com:6667 (eda2edb) 8902> 9798<
1744: 172.16.134.191:4828                     - 199.107.7.2:31337          (edc2edd) 3>   0<   (unidirectional)
1745: a66b8n163client125.hawaii.rr.com:3744   - 172.16.134.191:445         (ede2edf) 16>  13<  (complete)
1746: a66b8n163client125.hawaii.rr.com:3745   - 172.16.134.191:139         (edg2edh) 3>   1<   (reset)
1747: a66b8n163client125.hawaii.rr.com:3746   - 172.16.134.191:80          (edi2edj) 3>   2<
```

Le lecteur s'en rendra compte, la présentation claire et synthétique permet de prendre rapidement connaissance des échanges.

Conclusion partielle

Les événements journalisés sont représentatifs de l'activité 'anormale' quotidiennement constatée sur un quelconque équipement connecté sur un point d'accès INTERNET:

- Sondages des services classiques notamment ceux permettant d'identifier sans erreur possible un système Windows,
- Activité majoritairement en provenance d'adresses **IP** allouées dynamiquement par un **ISP** et correspondant à des accès de type **DialUp** ou **ADSL**.

On notera d'ores et déjà l'importante activité constatée sur le port '**UDP/1434**' correspondant très certainement aux tentatives de propagation du ver '**SQL Slammer**'. Pour aller plus loin dans l'analyse et détecter les tentatives réelles et effectives de compromission de la cible, nous allons devoir nous intéresser au contenu des sessions.

Etude des attaques

Deux outils peuvent nous aider dans cette démarche:

- '**tcpflow**' qui permet de reconstituer chacun des flux de données **TCP** échangés entres les différentes sources et destinations, les données étant stockées dans autant de fichiers qu'il y a de couples sources/destinations.
- '**snort**' qui permet de mettre rapidement en évidence les attaques autrement noyées dans la grande quantité d'événement enregistrés.

Utilisation de 'tcpflow'

La commande suivante permet d'engager l'analyse des flux **TCP** contenus dans le fichier '**sotm27**'.



```
# tcpflow –r sotm27 –s
```

Ceci conduit à la création de quelques **1164** fichiers dont **1031** correspondent aux données transmises vers la cible et **133** aux données transmises de la cible vers les systèmes externes. La taille de ces fichiers va de 8.2 Mo – un transfert WEB depuis le serveur '**users.mrf.va.web.rcn.net**' - à quelques kilo-octets.

Etant donnée la grande quantité d'informations à analyser, une démarche structurée va devoir être engagée qui va consister à analyser prioritairement les échanges pour lesquels les éléments statistiques laissent entendre qu'il puisse s'agir d'un trafic **TCP** anormal.

Les résultats de cette analyse 'purement' visuelle - donc uniquement basée sur l'expérience de l'investigateur - sont synthétisés dans le tableau suivant:

Connexions TCP sur la cible		
Adresse	**Cible**	**Activité**
24.197.194.106	80	Tentatives attaque UNICODE (885 variations)
210.22.204.101	80	Tentatives attaque MS01-033 dit '.ida' (71 tentatives)
	139	Sondage service NETBIOS
	445	Tentatives attaque SHARE SMB et installation produit FAMATECH Remote Administrator (fichiers 'r_server.exe', 'raddrv.dll', 'admdll.dll')
	4899	Accès FAMATECH Remote Administrator
129.116.182.239	445	Tentatives attaque SHARE SMB
66.139.10.15	445	Tentatives attaque SHARE SMB
209.45.125.69	445	Tentatives attaque SHARE SMB
61.111.101.78	445	Tentatives attaque SHARE SMB
195.36.247.77	445	Tentatives attaque SHARE SMB
213.23.49.158	445	Tentatives attaque SHARE SMB

Au prix d'un travail conséquent car purement manuel, nous avons ainsi pu mettre en évidence l'installation d'un outil d'administration distante sans pour autant avoir reconstitué une quelconque chronologie des évènements. Cette approche reste donc complexe et peu efficace par rapport à une inspection visuelle via '**ethereal**', du moins dans le cas d'une analyse portant sur un volume important de données.

Utilisation de 'snort'

La commande suivante permet d'engager l'analyse des flux contenus dans le fichier '**sotm27**' en ayant préalablement pris soin de configurer correctement le fichier '**snort.conf**'.

```
# snort –c ../etc/snort.conf –r sotm27
```

Une synthèse des alertes peut alors être rapidement obtenue en recherchant toutes les lignes commençant par la chaîne '**[****' dans le fichier '**alert**' généré par '**snort**'.

```
# grep '\[\*\*'alert
```

Nous obtenons ainsi une liste des 155 alertes qu'il va nous falloir étudier mais qui peuvent toutes être regroupées en 3 catégories:

Référence	Titre	Occurrences
1:2003:2	**MS-SQL Worm propagation attempt**	55
1:615:3	**SCAN SOCKS Proxy attempt**	1
100:2:1	**PORTSCAN DETECTED from 24.197.194.106**	86

Nous le constatons, si nous avons bien confirmation des tentatives d'accès dues au ver SQL Slammer (port **UDP/1434**) et du sondage réalisé par le système '**24.197.194.106**', aucune alerte n'apparaît concernant le problème du partage de fichier '**SMB**' précédemment identifié. Le lecteur aura probablement aussi remarqué l'absence de toute référence aux tentatives d'exploitation de la vulnérabilité '**.ida**'.

A cela deux raisons:

1. Le protocole SMB permettant le partage de fichier sur Internet (**TCP/445**) ne fait l'objet d'aucune règle prédéfinie puisque son utilisation ne peut être considérée comme une vulnérabilité mais tout au plus comme un problème de configuration,
2. Les tentatives d'exploitation du débordement de buffer présent dans le système d'index IIS ici caractérisées par la présence d'une requête du type '**GET NULL.IDA?CCCCCCCCCCCC**' sont comptabilisées en tant que sondage, aucune règle correspondant à la forme ici utilisée n'étant activée.

Dans le contexte présent, l'utilisation de '**snort**' n'apporte pas le gain escompté mais surtout ne permet pas de détecter le transfert du paquetage '**Remote Administrator**' par le biais du partage de fichier ouvert sur le service '**TCP/445**'.

Conclusion partielle

A ce stade de notre analyse et dans le contexte du défi, nous devons conclure qu'aucun des outils employés n'est pleinement satisfaisant. Nous allons donc devoir revenir à la méthode jusqu'à maintenant utilisée dans nos analyses: le parcours chronologique des échanges par le biais de l'outil '**ethereal**' en nous concentrant sur les points suivants:

1. Efficacité des sondages effectués par le système '**24.197.194.106**',
2. Condition d'utilisation du paquetage '**Remote Administrator**' installé depuis le système '**210.22.204.101**',
3. Recherche de toute autre tentative de compromission ayant pu conduit à l'activation du service IRC.

Analyse des événements



Les événements identifiés à la suite du parcours chronologique des échanges par le biais de l'outil '**ethereal**' vont être détaillés en nous concentrant sur les seuls éléments requis pour répondre aux questions du défi ou pertinents car mettant en avant un procédé ou une technique intéressante.

Evénements majeurs

Comme à notre habitude, nous référencerons ces évènements par le numéro du paquet associé.

Identification du système cible — 1 Mars 2003 – 10h08

Les deux premiers échanges journalisés correspondent à une requête '**Netbios Name Service**' transmise vers le service '**UDP/137**' de la cible et à la réponse transmise par celle-ci.

Trame	Source	Service	Donnée
1	219.118.31.42	UDP/137	Requête 'Name Query NBSTAT'
2	172.16.134.191		Réponse Nom=**PC0191** + divers paramètres
8	219.118.31.42	TCP/139	Requête 'Tree Connect AndX Request' vers \\PC0191\C

En un seul échange, le système distant à obtenu les informations '**NetBios**' nécessaires pour tenter d'engager d'autres conversations avec la cible. Dans le cas présent, le système tiers tente ensuite d'accéder – sans succès – au partage administratif correspondant au disque dur C: du système cible. On notera quelques 64 tentatives similaires sur la période journalisée en provenance d'autant de systèmes.

Identification du service WEB — 1 Mars 2003 – 10h08

Plusieurs connexions sur le service WEB (**TCP/80**) sont engagées qui permettent d'identifier le serveur utilisé.

Trame	Source	Service	Donnée
19	213.23.49.158	TCP/80	Requête 'HTTP HEAD'
25	172.16.134.191		Réponse 'Server :Microsoft-IIS/5.0' + divers paramètres

Tentatives d'attaque 'SQL SLAMMER' — 2 Mars 2003 – 00h27

Quelques 55 tentatives de propagation du code '**SQL Slammer**' ont été journalisées.

Trame	Source	Service	Donnée
104	206.149.148.192	UDP/1434	Code SQL Slammer

Accès distants à la base de registre — 4 Mars 2003 – 03h55

Plusieurs systèmes tiers accèdent – avec plus ou moins de succès - à la base de registre, et plus particulièrement aux informations de sécurité, par l'ouverture d'une connexion dite '**IPC anonyme**' puis association de cette connexion avec un quelconque outil d'accès **SMB**. Ce type d'attaque est en nette recrudescence depuis l'apparition d'outils – dont le ver **W32/Deloder** - permettant d'automatiser la recherche d'accès et l'installation de portes dérobées.

Trame	Source	Service	Donnée
287-292	195.36.247.77	TCP/445	Négociation du protocole SMB
293			Connexion IPC anonyme (\\172.16.134.192\IPC$)
295			Enumération de la base de registre
			Lecture de divers objets de la base de sécurité '**samr**'
418-422	195.36.247.77	TCP/445	Déconnexion

Mise en place d'un accès dérobé 'Remote Administration' — 5 Mars 2003 – 03h38/03h39

Parmi les systèmes précédents, le système '**210.22.204.101**' faire preuve d'une activité intense consistant d'abord à analyser la base de registre, puis à transférer le paquetage FAMATECH '**Remote Administration**' et enfin à lancer son exécution. Par défaut, ce produit utilise le port '**TCP/4899**' pour accueillir les sessions d'administration.

Trame	Source	Service	Donnée
919-924	210.22.204.101	TCP/445	Négociation du protocole SMB
925- …	210.22.204.101	TCP/445	Enumération de la base de sécurité
1188	210.22.204.101	TCP/445	Négociation du protocole SMB
1191- …	210.22.204.101	TCP/445	Multiples tentatives d'authentification
1364	210.22.204.101	TCP/445	Négociation du protocole SMB
1396- …	210.22.204.101	TCP/445	Transfert du fichier 'r_server.exe' vers '\Winnt\System32'
1649- …	210.22.204.101	TCP/445	Transfert du fichier 'raddrv.dll' vers '\Winnt\System32'
1688- …	210.22.204.101	TCP/445	Transfert du fichier 'admdll.dll' vers '\Winnt\System32'
1800- …	210.22.204.101	TCP/445	Exécution du fichier 'r_server.exe' en tant que service système
1821	210.22.204.101	TCP/445	Déconnexion

Il ne s'agit pas ici de l'activité des vers '**W32.Deloder**', '**W32/Slackdor**' ou '**W32/Lioten**' qui installent une porte dérobée différente. On notera cependant la similitude des traces journalisées avec du ver '**W32/Lioten**' dont une analyse est disponible sur le site 'http://www.mynetwatchman.com/kb/security/articles/iraqiworm/iraqitrace.htm'. Nous n'avons trouvé aucune trace d'un quelconque code ou ver utilisant le paquetage '**FAMATECH** Remote Administration'.

Une rapide étude du temps écoulé entre la première action – Trame 919 / 05 Mars 2003 – 3h38mn14s – et la finalisation de la compromission – Trame 1821 / 05 Mars 2003 – 3h39m23s – ne laisse aucun doute sur l'automatisation complète de l'attaque puisqu'il aura fallu à peine plus d'une minute pour ouvrir un accès dérobé, temps de transfert des trois fichiers compris !

Exploitation d'une vulnérabilité dans le service d'indexation — 5 Mars 2003 – 03h39/03h44



Immédiatement après l'activation de la porte dérobée, le système '**210.22.204.101**' continue son activité en tentant d'exploiter un débordement de buffer présent dans le service d'indexation d'IIS par le biais de diverses variations d'une même séquence d'attaque, chaque tentative étant immédiatement suivie d'un essai de connexion sur le port '**TCP/99**' qui échoue. On notera que la re-connexion sur le serveur **WEB** correspondant à la tentative d'attaque suivant n'est pas toujours immédiatement autorisée.

Trame	Source	Service	Donnée
1839	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
1845	210.22.204.101	TCP/99	Tentative de connexion: échoue
1849	210.22.204.101	TCP/80	Tentative de connexion WEB: échoue
1888	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
1892	210.22.204.101	TCP/99	Tentative de connexion : échoue
1898	210.22.204.101	TCP/90	Tentative de connexion WEB: échoue
1913	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
1917	210.22.204.101	TCP/99	Tentative de connexion : échoue
1925	210.22.204.101	TCP/90	Tentative de connexion WEB: échoue
1938	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
1942	210.22.204.101	TCP/99	Tentative de connexion : échoue
1948	210.22.204.101	TCP/90	Tentative de connexion WEB: échoue
1963	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
1974	210.22.204.101	TCP/99	Tentative de connexion : échoue
1981	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
1986	210.22.204.101	TCP/99	Tentative de connexion : échoue
1993	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
1997	210.22.204.101	TCP/99	Tentative de connexion : échoue
2004	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
2008	210.22.204.101	TCP/99	Tentative de connexion : échoue
2015	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
2019	210.22.204.101	TCP/99	Tentative de connexion : échoue
2026	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
2030	210.22.204.101	TCP/99	Tentative de connexion : échoue
2037	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
2041	210.22.204.101	TCP/99	Tentative de connexion : échoue
2037	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
2041	210.22.204.101	TCP/99	Tentative de connexion : échoue
2037	210.22.204.101	TCP/80	HTTP GET /NULL.ida?CCCCCCCCCC... cmd.exe ...
2041	210.22.204.101	TCP/99	Tentative de connexion : échoue

Les recherches menées sur Internet pour identifier le '**SHELLCODE**' activé par le débordement de buffer n'ont rien donné, d'autant que ce code semble être 'brouillé' pour éviter une lecture trop immédiate. Nous reconnaissons ne avoir eu le temps d'effectuer la rétro-analyse de celui-ci mais nous soupçonnons celui-ci d'ouvrir un accès permettant de passer des commande via le port **TCP/99**, comme le laisse entendre les nombreuses tentatives de connexion journalisées.

Exploitation de l'accès distant 'Remote Administration' 5 Mars 2003 – 03h44/03h48

L'accès ouvert par '**Remote Administration**' sur le port '**TCP/4899**' est ensuite exploité avec succès durant 4 minutes. A ce propos, la question se pose de savoir si les tentatives de connexion sur le port '**TCP/99**' précédemment mises en évidence ne proviendraient pas d'une erreur de configuration du l'outil d'attaque.

Trame	Source	Service	Donnée
2070	210.22.204.101	TCP/4899	Connexion sur le serveur '**Remote Administration**'
2080	210.22.204.101	TCP/4899	Fin de la connexion
2079	210.22.204.101	TCP/4899	Connexion sur le serveur '**Remote Administration**'
3087	210.22.204.101	TCP/4899	Rupture de la connexion sur le serveur '**Remote Administration**'

Nous nous heurtons maintenant à un problème de taille: le protocole d'échange utilisé par le produit de la société **FAMATECH** est tout particulièrement optimisé pour transférer la copie de l'écran du système distant et les actions effectuées en retour par l'utilisateur: déplacement de la souris, état des boutons, frappes clavier, …

En conséquence, les actions contenues dans les quelques 1003 paquets de la seconde session – 102Ko de données échangées - ne peuvent être déterminées et le contexte ne nous donne aucune information utile. On notera seulement qu'après cette session, plus aucun échange n'aura lieu entre le système '**210.22.204.101**' et la cible désormais considéré comme compromise.

Acquisition du paquetage 'swflash.cab' 5 Mars 2003 – 06h21/06h21

Le système cible se connecte sur le site '**64.0.96.9**' – une adresse allouée dans un bloc appartenant à '**XO Communications**', un **ISP** - pour télécharger le paquetage Macromedia '**swflash.cab**'. Une rapide analyse du contenu de ce paquetage fait apparaître la présence d'une signature Verisign confirmant son authenticité.

Trame	Source	Service	Donnée



3327	172.16.134.191	TCP/80	Téléchargement
3489	172.16.134.191	TCP/80	Fin du téléchargement

Cette activité n'apparaît donc pas être suspecte en l'état de l'analyse, tout comme la multitude d'accès WEB constatée dans les quelques 17000 paquets suivants.

Sondage actif du système cible **5 Mars 2003 – 11h42/11h46**

Une recherche systématique des services actifs sur le système cible est engagée par le système '**24.197.194.106**' sur les ports **TCP** classiques allant de 1 à 80 mais aussi sur les ports 110, 111, 139, 1433. On notera que service SSL est découvert actif.

Trame	Source	Service	Donnée
21001	24.197.194.106	TCP/1	Tentative de connexion : rejet
21003	24.197.194.106	TCP/2	Tentative de connexion : rejet
21306	24.197.194.106	TCP/xxx	Tentative de connexion : rejet

Recherche d'URL connues **5 Mars 2003 – 11h48/12h05**

Un sondage particulièrement actif – par ailleurs déjà détecté – est maintenant engagé par le système '**24.197.194.106**' à la recherche de la présence d'URL connues exploitables en environnement **IIS**.

Trame	Source	Service	Donnée
21373	24.197.194.106	TCP/80	'HTTP HEAD /'
21374	24.197.194.106	TCP/80	'HTTP HEAD /scripts/*.pl'
29635	24.197.194.106	TCP/80	'HTTP HEAD /scripts/check.bat/..\../..\winnt/system32/cmd.exe …'
30324	24.197.194.106	TCP/80	'HTTP POST /index.asp'

Tentatives d'exploitation d'un débordement de buffer **5 Mars 2003 – 12h05/12h10**

Ce même système '24.197.194.106' tente ensuite d'exploiter le débordement de buffer associé au serveur d'index IIS mais sans aucun succès.

Trame	Source	Service	Donnée
30461	24.197.194.106	TCP/80	'HTTP GET /NULL.printer'
30462	24.197.194.106	TCP/80	'HTTP GET /NULL.ida?AAAAAAAAAA…..'
30888	24.197.194.106	TCP/80	'HTTP GET /NULL.ida?AAAAAAAAAA…..'

Tentative d'attaque 'CODE RED' **6 Mars 2003 – 00h24**

Le système '218.25.147.83' est infecté par le ver '**Code Red**' qui tente de se propager sans grand succès.

Trame	Source	Service	Donnée
32885-9	218.25.147.83	TCP/80	'HTTP GET /default.ida?NNNNNNNN … hacked by chinese …'

Tentative d'installation du serveur d'accès 'psexec' **6 Mars 2003 – 04h35/04h38**

Le système '**61.111.101.78**' utilise la technique de l'ouverture d'un partage 'anonyme' pour installer le service '**PSExeSvc.exe**' puis tente activer celui-ci via une commande **RPC**. Parfaitement documenté sur le site 'NtKernel' à la page accessible via '**http://www.ntkernel.com/articles/psexec.shtml**', ce service se comporte comme un point d'accès distant permettant le passage de commandes par le biais d'une connexion **SMB** ouverte à destination de plusieurs '**Pipe Nommé**', un '**telnet**' pour Windows en quelque sorte.

Trame	Source	Service	Donnée
33328	61.111.101.78	TCP/445	Négociation du protocole SMB
33237	61.111.101.78	TCP/445	Enumération de la base de sécurité
33262	61.111.101.78	TCP/445	Négociation du protocole SMB
33280	61.111.101.78	TCP/445	Transfert du fichier 'psexesvc.exe' vers '\System32'
33375	61.111.101.78	TCP/445	Tentative d'exécution de '%SYSTEMROOT\System32\psexesvc.exe'
33480	61.111.101.78	TCP/445	Relecture du fichier 'psexesvc.exe'
33533	61.111.101.78	TCP/445	Destruction du fichier '\System32\psexesvc.exe'
33537	61.111.101.78	TCP/445	Transfert du fichier 'psexesvc.exe' vers '\System32'
33678	61.111.101.78	TCP/445	Transfert du fichier 'inst.exe' vers '\System32'
34500	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
34504	61.111.101.78	TCP/445	Destruction du fichier '\System32\psexesvc.exe'
34508	61.111.101.78	TCP/445	Transfert du fichier 'psexesvc.exe' vers '\System32'
34590	61.111.101.78	TCP/445	Tentative d'exécution de '%SYSTEMROOT\System32\psexesvc.exe'
34670	61.111.101.78	TCP/445	Tentative de transfert de '\System32\psexesvc.exe'
34679	61.111.101.78	TCP/445	Tentative d'exécution de '%systemeroot%\System32\psexesvc.exe'
34741	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
34743	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
34745	61.111.101.78	TCP/445	Destruction du fichier '\System32\psexesvc.exe'
34749	61.111.101.78	TCP/445	Transfert du fichier 'psexesvc.exe' vers '\System32'
34831	61.111.101.78	TCP/445	Tentative d'exécution de %systemeroot%\System32\psexesvc.exe'
34839	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
34841	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
34943	61.111.101.78	TCP/445	Destruction du fichier '\System32\psexesvc.exe'
34947	61.111.101.78	TCP/445	Transfert du fichier 'psexesvc.exe' vers '\System32'
35030	61.111.101.78	TCP/445	Tentative d'exécution de %systemeroot%\System32\psexesvc.exe'



35138	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
35140	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
35142	61.111.101.78	TCP/445	Destruction du fichier '\System32\psexesvc.exe'
35146	61.111.101.78	TCP/445	Transfert du fichier 'psexesvc.exe' vers '\System32'
35228	61.111.101.78	TCP/445	Tentative d'exécution de %systemeroot%\System32\psexesvc.exe'
……..	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
……..	61.111.101.78	TCP/445	Vérification présence du fichier '\System32\psexesvc.exe'
……..	61.111.101.78	TCP/445	Destruction du fichier '\System32\psexesvc.exe'
……..	61.111.101.78	TCP/445	Transfert du fichier 'psexesvc.exe' vers '\System32'
……..	61.111.101.78	TCP/445	Tentative d'exécution de %systemeroot%\System32\psexesvc.exe'
35738	61.111.101.78	TCP/445	Clôture du protocole SMB

On constatera à la lecture des éléments précédents que l'attaquant n'arrive pas à initialiser le service après qu'il l'ait pourtant correctement transféré. Il abandonne après maints essais, sans s'être aperçu de son erreur : le chemin d'accès utilisé pour sauvegarder le fichier est incorrect.

Cas particulier des accès IRC

Les accès IRC sont majoritairement regroupés en fin de journalisation en date du 6 mars aux environs de 4h45 du matin. Ceci sous-entend que le client '**IRC**' a probablement été installé lors de l'une des compromissions précédentes. L'analyse menée précédemment ne permettant pas d'identifier une quelconque séquence d'installation d'un script 'IRC' ou d'un exécutable spécifique, nous supposerons que cette installation a été initialisée en dehors de la période de journalisation ou bien a été effectuée par le biais du serveur d'administration distant '**Remote Administration**'.

Conversations IRC — 6 Mars 2003 – 04h36 / 09h27

Le système compromis tente d'initialiser sans succès une première session **IRC** vers les systèmes '209.126.161.29' et '66.33.65.58'.

Trame	Cible	Service	Donnée
34821	209.126.161.29	TCP/6667	04:36 Tentative d'ouverture
35739	66.33.65.58	TCP/6667	04:45 Tentative d'ouverture

Quelques minutes plus tard, une seconde session est engagée avec succès cette fois-ci vers le système '63.241.174.144'.

35745	63.241.174.144	TCP/6667	04:56 Ouverture session IRC
35761	63.241.174.144	TCP/6667	04:56 Fin de session IRC

La conversation journalisée montre que le programme installé sur le système compromis tente d'utiliser un '**pseudo**' ou '**nickname**' déjà utilisé sur le réseau '**IRC**' auquel est rattaché le système distant.

```
<- NOTICE AUTH :*** Looking up your hostname...
<- NOTICE AUTH :*** Checking Ident
<- NOTICE AUTH :*** No Ident response
-> NICK eohisou
   USER eohisou localhost localhost :eohisou
<- NOTICE AUTH :*** Found your hostname: irc4.aol.com 433
                  * eohisou :Nickname is already in use.
         ERROR :Closing Link: [eohisou@255.255.255.255] (Connection Timed Out)
```

Une troisième session est ensuite engagée vers le système '217.199.175.10'.

35762	217.199.175.10	TCP/6667	04:56 Ouverture session IRC
35775	217.199.175.10	TCP/6667	04:56 Fin de session IRC

La conversation journalisée montre que cette fois, la connexion est refusée car le serveur distant est saturé. On notera que les pseudos sont vraisemblablement générés aléatoirement par le programme de '**bot**'.

```
<- NOTICE AUTH :*** Looking up your hostname...
<- NOTICE AUTH :*** Checking Ident
<- NOTICE AUTH :*** No Ident response
-> NICK rgdiuggac
   USER rgdiuggac localhost localhost : rgdiuggac
<- ERROR :Closing Link: rgdiuggac[~rgdiuggac@255.255.255.255] (Sorry server is full –
          try later)
```

La session suivante est engagée vers le système '209.126.161.29' qui ne répond pas, puis de nouveau vers le système '66.33.65.58' tout aussi muet et enfin vers le système '209.196.44.172' sur lequel une conversation est enfin établie.

35794	209.196.44.172	TCP/6667	05:23 Ouverture session IRC
54536	209.196.44.172	TCP/6667	09:27 Fin de session IRC

Cette conversation qui dure plus de 4 heures contient les différentes actions couramment effectuées par les 'robots' IRC chargés de maintenir le contrôle et l'activité d'un ensemble de canaux. Nous allons en étudier les principales sections, le volume d'échange – 548 lignes – étant trop important pour en analyser chaque élément.

```
<- NOTICE AUTH :*** Looking up your hostname...
<- NOTICE AUTH :*** Checking Ident
<- NOTICE AUTH :*** No Ident response
-> NICK rgdiuggac
-> USER rgdiuggac localhost localhost : rgdiuggac
```



```
<- :irc5.aol.com 001 rgdiuggac :Welcome to the Internet Relay Network rgdiuggac
<- :irc5.aol.com 002 rgdiuggac :Your host is irc5.aol.com[irc5.aol.com/6667], running
                                version 2.8/hybrid-6.3.1
```

Le 'robot' se connecte correctement sur le serveur **IRC** distant en s'annonçant sous le pseudo '**rgdiuggac'**. On notera que le serveur s'annonce '**irc5.aol.com**' alors qu'une recherche sur l'adresse '209.196.44.172' nous indique qu'il s'agit du système '**ipdwbc0271atl2.public.registeredsite.com**'. Nous ne pouvons qu'envisager que ce système agisse en tant que relais vers le réseau **IRC AOL**.

```
<- :irc5.aol.com 003 rgdiuggac :This server was created Sun Jan 19 2003 at 19:04:03 PST
<- :irc5.aol.com 004 rgdiuggac irc5.aol.com 2.8/hybrid-6.3.1 oOiwszcrkfydnxb biklmnopstve
<- :irc5.aol.com 005 rgdiuggac WALLCHOPS PREFIX=(ov)@+ CHANTYPES=#& MAXCHANNELS=20
                               MAXBANS=25 NICKLEN=9 TOPICLEN=120 KICKLEN=90 NETWORK=Xnet
                               CHANMODES=be,k,l,imnpst EXCEPTS KNOCK MODES=4 :
                               are supported by this server
<- :irc5.aol.com 251 rgdiuggac :There are 0 users and 4752 invisible on 4 servers
<- :irc5.aol.com 252 rgdiuggac :1 IRC Operators online
<- :irc5.aol.com 254 rgdiuggac :4 channels formed
<- :irc5.aol.com 255 rgdiuggac :I have 346 clients and 1 servers
<- :irc5.aol.com 265 rgdiuggac :Current local  users: 346  Max: 348
<- :irc5.aol.com 266 rgdiuggac :Current global users: 4752  Max: 4765
<- :irc5.aol.com 250 rgdiuggac :Highest connection count: 349 (348 clients)
                                (378 since server was (re)started)
<- :irc5.aol.com 375 rgdiuggac :- irc5.aol.com Message of the Day -
<- :irc5.aol.com 372 rgdiuggac :- - WELCOME TO AMERICA ONLINE'S - IRC SERVER
<- :irc5.aol.com 372 rgdiuggac :-
<- :irc5.aol.com 372 rgdiuggac :- - !!!   WARNING WARNING WARNING WARNING   !!!
<- :irc5.aol.com 372 rgdiuggac :- - !!!  THIS SERVER SCANS FOR OPEN PROXIES !!!
<- :irc5.aol.com 372 rgdiuggac :- - !!!    PORTS: 8080,3128,80,1080,23      !!!
<- :irc5.aol.com 372 rgdiuggac :- -   So if this is a legal problem in your
<- :irc5.aol.com 372 rgdiuggac :- -     country please disconnect NOW!
<- :irc5.aol.com 372 rgdiuggac :- -  We do this to make your IRC experience
<- :irc5.aol.com 372 rgdiuggac :- -  more enjoyable.
<- :irc5.aol.com 376 rgdiuggac :End of /MOTD command.
```

Le serveur informe ensuite l'utilisateur qu'il est accueilli en tant qu'invité (MODE +i).

```
<- :rgdiuggac MODE +i
```

Le 'robot' cherche à joindre le canal '**xàéüîéðìx**' et demande la liste des utilisateurs actuellement connectés sur celui-ci.

```
-> MODE rgdiuggac –x
-> MODE rgdiuggac +i
-> JOIN #xàéüîéðìx :sex0r
-> WHO  rgdiuggac
```

Le serveur IRC confirme la requête d'accueil sur le canal '**xàéüîéðìx**' et retourne une impressionnante liste de **6918 pseudonymes** dont la constitution confirme qu'il s'agit d'identités employées par d'autres 'robots' IRC utilisant le canal '**xàéüîéðìx**' comme moyen de communication. Ce '**botnet**' est en conséquence constitué d'au moins **6918+1** systèmes …

```
<- :rgdiuggac!~rgdiuggac@pc0191.example.com JOIN :#xàéüîéðìx
<- :irc5.aol.com 353 rgdiuggac @ #xàéüîéðìx : rgdiuggac mikeoof   riktgisli moongihli ...
<- :irc5.aol.com 353 rgdiuggac @ #xàéüîéðìx : aloncoseb rrscbfgzz radlmonid mibecoohd ...
                                       ......
<- :irc5.aol.com 353 rgdiuggac @ #xàéüîéðìx : mhowugxb  piwhpzni  rosgmivpa moonoonic ...
<- :irc5.aol.com 353 rgdiuggac @ #xàéüîéðìx : End of /NAMES list.
```

Le 'robot' ayant rejoint le canal du '**botnet**' sera maintenant informé de toutes les actions de ses semblables. Ici, trois 'robots' n'ont pas répondu à la demande de confirmation de présence (PING/PONG) et sont donc déconnectés du canal.

```
<- :gercgirld!~gercgirld@211.105.132.47 QUIT :Ping timeout: 600 seconds
<- :redykkyz!~redykkyz@218.98.84.210 QUIT :Ping timeout: 600 seconds
<- :stehfon!~stehfon@137.141.244.169 QUIT :Ping timeout: 600 seconds
```

Quelques instants plus tard nous apprenons que plusieurs nouveaux robots viennent de se connecter :

```
<- :moinoonik!~moinoonik@61.111.228.17 JOIN :#xàéüîéðìx
<- :oiwigfrl!~oiwigfrl@host34.2106211.gcn.net.tw JOIN :#xàéüîéðìx
<- :mikemrrh!~mikemrrh@dyn33-37.sftm-212-159.plus.net JOIN :#xàéüîéðìx
```

Les quelques 500 lignes suivantes sont similaires et contiennent l'activité du canal '**xàéüîéðìx**' permettant au '**botnet**' de communiquer. L'analyse de ces échanges permet d'obtenir une liste assez complète des adresses IP des systèmes sur lequel un '**robot**' a été installé ainsi que le pseudonyme utilisé par ce robot.

Un script d'analyse écrit pour l'occasion nous permet d'établir une liste de **366 systèmes actifs** sur le canal durant la période de journalisation dont une extrait est proposé ci-après.

Pseudo	Serveur	JOIN	QUIT
~aaxcbgl	218.98.81.236		
~aeepmoni	bgp377180bgs.plnfld01.nj.comcast.net		
~aikeceeed	210.38.34.51		
~aiketoniq	210.3.14.84		



~aoaxgirl	E137209.ppp.dion.ne.jp	X	
~aocabopo	220.83.28.15		
~aotigir	61.96.27.50	X	
~aswinvrl	218-167-24-116.HINET-IP.hinet.net		
~atonmibh	211.139.7.69		
~axrctic	218.71.2.141		
~bikemichk	211.144.115.228	X	
~bockqah	210.77.114.82	X	
~bohsmoni	...-227.nas26.austin2.tx.us.da.qwest.net		
~brlfgir	210.113.49.118		
~capaboyz	cae88-96-118.sc.rr.com		
~cemfpik	210.5.9.105		
~cikebocsz	177.c30.ethome.net.tw	X	X
~wolfcokpd	218.55.23.179		X
~wolflrund	218.236.6.211		X
~wolfpop	211.204.69.128	X	
~wolfsoubh	211.175.1.168	X	X
~wolfuglq	246.c11.ethome.net.tw		X
~wolnmoy	61.52.19.7		X
~woloiok	218.98.96.106	X	
~wolonoai	cpe-066-061-020-032.midsouth.rr.com	X	

Réponse aux questions

Arrivé à ce niveau de l'analyse, nous disposons de la majorité des éléments permettant de répondre aux questions:

Niveau débutant

1. *Qu'est ce que IRC ?*

Sigle de **I**nternet **R**elay **C**hat, '**IRC**' peut être considéré comme le descendant de l'utilitaire UNIX '**talk**' qui permettait à plusieurs utilisateurs de discuter par le biais d'un écran divisé en autant de fenêtres qu'il y avait d'interlocuteurs connectés. En pratique, '**IRC**' prend la forme d'une véritable infrastructure de diffusion d'information dans laquelle tout message transmis par un client vers son serveur de rattachement sera immédiatement redistribué vers l'ensemble des serveurs constituant le réseau '**IRC**'. Ce message sera diffusé à tous les clients ayant rejoint le groupe de discussion – ou '**channel**' dans le jargon – dans lequel il a été émis.

On compte à l'heure actuelle une quinzaine de grands réseaux **IRC** officiels non interconnectés et actuellement en activité. Citons **EFFNet**, le réseau historique, **IRCNet**, **AOL**, **Microsoft**, **Undernet**, **DalNet** mais aussi de nombreux réseaux pouvant être qualifiés de 'privés'.

2. *Quel est le message transmis par IRC pour rejoindre le réseau ?*

Après s'être connecté sur un serveur **IRC** via une session ouverte généralement sur le port '**TCP/6667**', l'utilisateur devra mentionner le ou les canaux de discussion qu'il souhaite rejoindre. En pratique, l'utilisateur aura préalablement choisi un pseudonyme – ou 'nickname' – unique dans le réseau IRC utilisé. Après validation de ce pseudonyme par le serveur, l'utilisateur pourra utiliser les commandes à sa disposition pour obtenir la liste des canaux de discussion publics et éventuellement rejoindre l'un de ces canaux par le biais de la commande '**JOIN**'.

La particularité du réseau **IRC** réside dans un choix de conception remarquable consistant à rendre totalement dynamique la création d'un canal: la première personne activant la commande '**JOIN**' sur le nom d'un canal inexistant en devient l'administrateur – le **sysop** - c'est à dire la personne ayant toute autorité sur les futurs utilisateurs de ce canal.

La durée de vie d'un canal est directement liée à la présence d'au moins un utilisateur actif sur celui-ci. Un administrateur quittant son canal par la commande '**QUIT**' perdra immédiatement son privilège au détriment de l'utilisateur suivant dans la liste des connexions à moins qu'il n'ait délégué cette autorité à un autre utilisateur (ou à lui même par le biais d'un autre pseudonyme !). Lorsque tous les utilisateurs d'un canal ont quitté celui-ci, ce canal pourra de nouveau être ré-attribué.

3. *Qu'est ce qu'un 'botnet' ?*

Le mode de fonctionnement de l'**IRC** a très rapidement conduit à une véritable guérilla virtuelle dont l'objet est la conservation ou la prise de contrôle des canaux qu'ils soient publics – et normalement maintenus actifs – ou privés et accessibles sur invitation. Les procédés permettant de conserver le contrôle d'un canal ont évolués au fur et à mesure de l'accroissement de l'Internet. Initialement, ce contrôle était assuré par le biais de '**scripts**' régulièrement activés par les clients IRC afin de maintenir une activité minimale sur le canal.

Les limitations inhérentes à ce procédé – perte du canal en cas d'arrêt du client ou de rupture de la connexion – ont conduit à développer un système coopératif et distribué constitué d'agents appelés '**bots**' – en référence au terme '**robot**' - agissant en tant qu'opérateurs systèmes pour assurer le maintien des canaux mais aussi pour imposer une certaine forme de police en bannissant les utilisateurs qui ne respecteraient pas les règles d'utilisation édictées par les créateurs de ces canaux.

4. *Quelle est généralement l'utilité d'un 'botnet' ?*

Poussée à l'extrême, cette logique a donnée naissance à des réseaux de '**bots**', les '**botnets**', utilisant les mécanismes offerts par '**IRC**' pour communiquer entre eux et disposant de multiples fonctionnalités activables par le biais de commandes spécifiques transmises dans des canaux IRC dédiés à la communication entre '**bots**'. Chaque '**bot**' devient alors un agent susceptible d'être activé à distance pour engager une action quelconque, un déni de service par exemple. La capacité de contrôle des canaux IRC – et plus largement de l'Internet – étant



directement liée à la taille du '**botnet**' chargé de leur gestion, il est de plus en plus fréquent de créer ces réseaux de contrôle à partir de milliers de systèmes répartis de par le monde et disposant si possible d'interconnexions de qualité.

Deux solutions sont couramment utilisées:

- utilisation de systèmes personnels connectés à l'Internet via l'**ADSL** ou le câble avec le risque de voir son système à son tour attaqué pour prendre le contrôle des canaux,
- installation systématique d'agents sur une majorité de systèmes tiers en exploitant toutes les vulnérabilités possibles. A l'heure actuelle, le procédé le plus utilisé consiste à transporter l'agent en tant que charge utile d'un ver ou d'un virus. Tout système compromis ou contaminé devient immédiatement et involontairement un nœud actif d'un '**botnet**'.

A ce propos, nous conseillons la lecture du remarquable article publié en 1996 sous le titre '**Bots are Hots**' dans '**Wired Magazine**' concernant le bestiaire rencontré sur **IRC** ainsi que de l'avis CERT **CA-2003-8**.

5. Quels sont les ports couramment utilisés par IRC ?

La connexion sur un serveur IRC est généralement engagée par défaut sur le port **TCP/6667** la plage **TCP/6660** à **TCP/6669** étant considérée réservée à cette application. Ceci étant, certains réseaux IRC offrent un accès sur d'autres ports dont le port **TCP/7000**.

6. Qu'est ce qu'un fichier de journalisation binaire et comment est-il créé ?

La majorité des outils d'analyse réseau, de détection d'intrusion et de surveillance enregistrent les évènements pertinents dans un(des) fichier(s) dits de journalisation. Le format employé dépend de l'application ayant généré ce fichier mais il est d'usage que les données enregistrées le soit dans un format concis afin de réduire le volume des journaux. Ainsi, dans le cas des journaux générés par les outils '**tcpdump**' et '**snort**', une option est proposée qui conduit à l'enregistrement des structures pertinentes dans un format 'binaire' donc non lisible par une être humain.

7. Avec quels serveurs IRC le système compromis dont l'adresse est 172.16.134.191 communique-t-il ?

Nous avons observé à partir de la trame '35739' plusieurs tentatives de connexion vers les serveurs IRC suivants:

Adresse IP	Nom DNS		Résultats	Essais
209.126.161.29	ISP CARI	- pas de nom	Pas de réponse	9
66.33.65.58	DNS	- ns.espaciosweb.net	Pas de réponse	9
63.241.174.144	CERFnet	- Pas de nom	Erreur pseudo	1
217.199.175.10	DNS	- ns2.caralarmuk.com	Serveur saturé	1
209.196.44.172	ISP SPRINT	- ipdwbc0271atl2.public.registeredsite.com	Activité	1

L'application du filtre suivant sur les trames présentées par l'outil '**Ethereal**' permet de confirmer qu'aucun système n'a été oublié dans notre analyse:

Système compromis		établissant une session TCP (flag SYN)		vers IRC
ip.src eq 172.16.134.191	and	tcp.flags.syn eq 1 and tcp.flags.ack eq 0	and	tcp.dstport eq 6667

8. Sur la période d'analyse, combien de systèmes ont accédé le 'botnet' via 209.196.44.172 ?

L'étude des 548 lignes correspondant aux messages transmis par le serveur IRC '**209.196.44.172**' à destination du système compromis nous a permis d'identifier 6918+1 pseudonymes donc probablement autant d'agents, l'analyse détaillée des adresses ayant conduit à identifier **366** systèmes actifs distincts.

9. En considérant que chaque nœud dispose d'un lien de 56Kps, quelle est la bande passante du botnet ?

Au maximum, 6919 systèmes communiquent avec le serveur **IRC** du botnet dont 366 durant la période d'analyse. Sans analyser en détail l'activité de connexion/déconnexion de chacun de ces systèmes sur cette période, nous pouvons estimer la bande passante utilisée à **20Mo/s** (366*56Kbps).

Niveau intermédiaire

1. Quelles sont les adresses IP sources utilisées pour attaquer le pot de miel ?

Nous avons identifié en début d'analyse 77 adresses IP différentes ayant tenté d'accéder au pot de miel via le protocole **TCP** et 113 via le protocole **UDP**. Un lissage de ces deux tables nous conduit à identifier **190 adresses distinctes**. En regard des services cibles, nous pouvons considérer que la majorité de ces adresses ont un comportement suspect.

2. Quelles vulnérabilités les attaquants ont-ils tenté d'exploiter ?

Durant notre analyse, nous avons relevé les tentatives d'exploitation des vulnérabilités ou des défauts de configuration suivant:

Sondage du service NETBIOS UDP/137

Ceci n'est pas à proprement parler une vulnérabilité mais un problème de configuration du filtrage permettant l'obtention d'informations utiles pour les phases ultérieures d'une attaque. Quelques <u>65 tentatives</u> ont été relevées. Le filtre '**ethereal**' suivant peut être utilisé pour mettre en évidence ces tentatives.

Système cible		vers UDP/137
ip.dst eq 172.16.134.191	and	udp.dstport eq 137

Débordement de buffer SQL UDP /1434

Toutes les tentatives enregistrées correspondent au mécanisme de propagation du ver '**SQL Slammer**'. Les <u>55 systèmes</u> à l'origine de ces tentatives sont donc tous infectés. Le filtre '**ethereal**' suivant peut être utilisé pour mettre en évidence ces tentatives.

Système cible		vers UDP/1434
ip.dst eq 172.16.134.191	and	udp.dstport eq 137



Sondage du service WEB TCP/80

Parmi les 1107 connexions effectuées sur le service WEB, on remarquera deux catégories de connexions visant explicitement à attaquer le système cible: une recherche systématique d'URL connues pour être exploitables en environnement IIS (système '24.97.194.106') et plusieurs tentatives d'exploitation du débordement de buffer présent dans le service d'indexation '**.ida**' (système '210.22.204.101'). On notera enfin une connexion de la part du système '218.25.147.83' infecté par le ver '**CodeRed**'.

Système cible		vers TCP/80		avec tentative d'établir une session
ip.dst eq 172.16.134.191	and	tcp.dstport eq 80	and	tcp.flags.syn eq 1 and tcp.flags.ack eq 0

Sondage du service NETBIOS TCP/139

La majorité des 84 connexions relevées sur ce service visent à tenter d'établir une session anonyme dite 'NULL SESSION' pour ensuite engager une session **NetBios/SMB**.

Système cible		vers TCP/139		avec tentative d'établir une session
ip.dst eq 172.16.134.191	and	tcp.dstport eq 139	and	tcp.flags.syn eq 1 and tcp.flags.ack eq 0

Sondage du service SMB TCP/445

La majorité des 19 connexions sur ce service actif sur la cible ont pour objet d'utiliser les services SMB dont notamment le partage des volumes du système cible sur le réseau. On ne peut ici parler de vulnérabilité mais seulement de problème de configuration.

Système cible		vers TCP/445		avec tentative d'établir une session
ip.dst eq 172.16.134.191	and	tcp.dstport eq 445	and	tcp.flags.syn eq 1 and tcp.flags.ack eq 0

Sondage du service SQL TCP/1433

La majorité des 23 tentatives de connexions sur ce service – inactif sur la cible - visent probablement à tenter d'exploiter l'accès au compte '**sa**' du serveur SQL.

Système cible		vers TCP/1433		avec tentative d'établir une session
ip.dst eq 172.16.134.191	and	tcp.dstport eq 1433	and	tcp.flags.syn eq 1 and tcp.flags.ack eq 0

3. Quelles ont été les attaques réussies ?

A priori, et sauf erreur d'analyse, une seule attaque semble avoir réussie: celle engagée par le système '210.22.204.101', un système utilisant une adresse localisée dans un bloc appartenant à '**TECH GROUP CNC**', une société domiciliée à Beijing en Chine. En exploitant la possibilité d'accéder aux volumes de stockage du système cible par le biais des partages administratifs, l'attaquant a pu installer un outil de prise de contrôle à distance '**Remote Administration V2.0**'. Les actions engagées par l'intermédiaire de cet accès n'ont hélas pu être déterminées de par la nature du protocole utilisé.

Conclusion

Notre analyse peut paraître complexe et longue mais nous avons volontairement choisi d'utiliser plusieurs approches pour mettre en avant les avantages et inconvénients de chacune. Nous aurions pu aller immédiatement à l'essentiel en utilisant une version de '**snort**' configurée et optimisée – ou de tout autre outil offrant une fonction de recherche de signature d'attaque - pour l'analyse a posteriori de journaux.

Dans le monde réel, une telle analyse aurait été facilitée par la possibilité d'étudier en détail le système compromis pour y rechercher d'autres traces et indices. Cependant, rares sont les environnements de 'production' pour lesquels la totalité des échanges sont journalisés. Nous aurions donc probablement été confronté à l'absence de nombreuses traces réseaux forts utiles pour reconstituer avec précision le cheminement de l'attaque.

Pour conclure, nous conseillons la lecture de l'article publié le 9 avril sur **ZDNET** par les chercheurs de l'université d'**AZULA** ayant proposé ce défi, article confirmant notre analyse.

▪ **Complément d'information**

http://project.honeynet.org/scans/scan27/

http://www.cert.org/advisories/CA-2003-08.html

http://www.wired.com/wired/archive/4.04/netbots_pr.html

http://www.zdnet.com.au/newstech/security/story/0,2000024985,20273555,00.htm